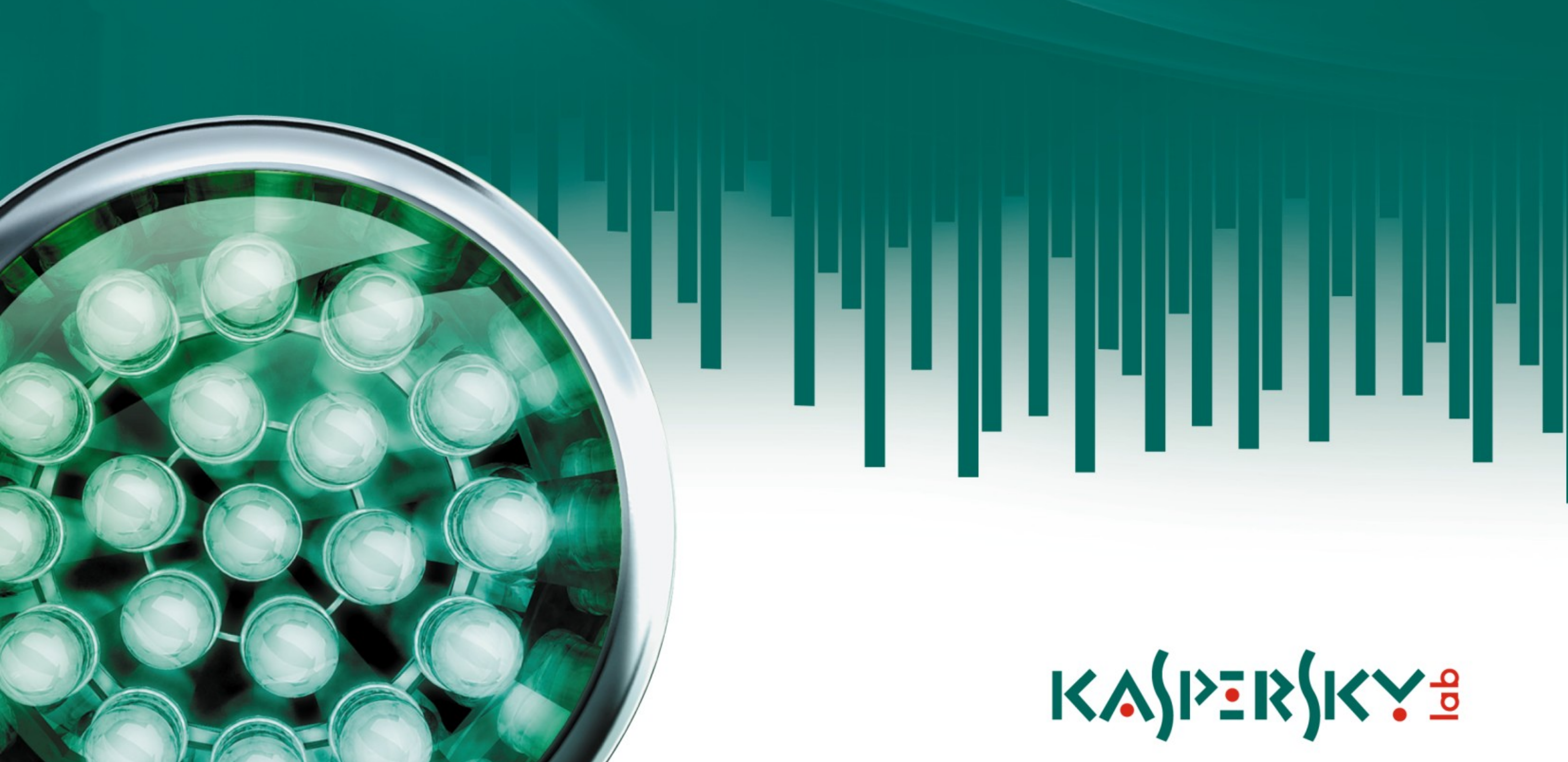
Kaspersky Password Manager

BENUTZERHANDBUCH



Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass dieses Handbuch Ihnen hilft und die meisten Fragen damit beantwortet werden können.

Das Dokument darf ohne vorherige Benachrichtigung geändert werden. Die neueste Version finden Sie auf der Seite von Kaspersky Lab unter der Adresse http://www.kaspersky.com/de/docs.

Redaktionsdatum: 19.10.2010

http://www.kaspersky.de
http://support.kaspersky.com/de/

INHALT

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE FOLGENDE RECHTLICHE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

INDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE „AKZEPTIEREN“ KLICKEN ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEBEN, ERKLÄREN SIE SICH MIT DER EINHALTUNG DER GESCHÄFTSBEDINGUNGEN DIESES VERTRAGS EINVERSTANDEN. **DIESE AKTION KONSTITUIERT EIN BEKENNTNIS IHRER SIGNATUR UND SIE STIMMEN DIESER VEREINBARUNG, UND DASS SIE EINE PARTEI DIESER VEREINBARUNG WERDEN, ZU UND ERKLÄREN SICH WEITERHIN EINVERSTANDEN, DASS DIESE VEREINBARUNG, WIE JEDWEDE ANDERE SCHRIFTLICHE, AUSGEHANDELTE UND DURCH SIE UNTERZEICHNETE VEREINBARUNG AUCH, VOLLSTRECKBAR IST.** SOLLTEN SIE MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SEIN, BEENDEN SIE DIE INSTALLATION DER SOFTWARE BZW. INSTALLIEREN SIE SIE NICHT.

NACHDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE „AKZEPTIEREN“ GEKLICKT ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEGEBEN HABEN, SIND SIE BERECHTIGT, DIE SOFTWARE IM EINKLANG MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG ZU NUTZEN.

1. <u>Definitionen</u>

1.1. **Software** bezeichnet Software einschließlich aller Updates und zugehöriger Materialien.

1.2. **Rechtsinhaber** (Inhaber aller Rechte an der Software, ob exklusiv oder anderweitig) bezeichnet Kaspersky Lab ZAO, ein gemäß den Gesetzen der Russischen Föderation amtlich eingetragenes Unternehmen.

1.3. **Computer** bezeichnet/bezeichnen Hardware, einschließlich von PCs, Laptops, Workstations, PDAs, Smart Phones, tragbaren oder sonstigen elektronischen Geräten, für welche die Software konzipiert war und auf denen die Software installiert und/oder verwendet werden wird.

1.4. **Endnutzer (Sie)** bezeichnet eine bzw. mehrere Personen, die die Software in eigenem Namen installieren oder nutzen, oder die eine Software-Kopie rechtmäßig nutzt/nutzen, oder, falls die Software im Namen einer Organisation heruntergeladen oder installiert wurde, wie etwa einem Arbeitgeber, bezeichnet der Begriff *„Sie“* weiterhin jene Organisation, für die die Software heruntergeladen oder installiert wird, und es wird hiermit erklärt, dass eine solche Organisation die diese Vereinbarung akzeptierende Person autorisiert hat, dies in ihrem Namen zu tun. Im Sinne dieses Lizenzvertrags beinhaltet der Begriff *„Organisation“* ohne Einschränkungen jedwede Partnerschaft, GmbH, Gesellschaft, Vereinigung, Aktiengesellschaft, Treuhandgesellschaft, Gemeinschaftsunternehmen, Arbeitsorganisation, nicht eingetragene Organisation oder staatliche Behörde.

1.5. **Partner** bezeichnet Organisationen oder Personen, die die Software auf Grundlage eines Vertrags und einer mit dem Rechtsinhaber vereinbarten Lizenz vertreiben.

1.6. **Update(s)** bezeichnet/n alle Upgrades, Korrekturen, Patches, Erweiterungen, Reparaturen, Modifikationen, Kopien, Ergänzungen oder Wartungs-Softwarepakete usw.

1.7. **Benutzerhandbuch** bezeichnet die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

2. <u>Lizenzgewährung</u>

2.1. Der Rechtsinhaber gewährt Ihnen hiermit eine nicht-ausschließliche unbefristete Lizenz zur Speicherung, zum Laden, zur Installation, Ausführung und Darstellung (zur „Nutzung“) der Software auf einer festgelegten Anzahl von Computern zur Nutzung der Software gemäß der Angaben im Nutzerhandbuch, gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen und im Einklang mit den Geschäftsbedingungen dieses Vertrags (die „Lizenz“). Sie erkennen diese Lizenz an.

Testversion. Sollten Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert haben und sollte Ihnen hiermit eine Evaluierungslizenz für die Software gewährt worden sein, dürfen Sie die Software ab dem Datum der ersten Installation nur zu Evaluierungszwecken verwenden, und zwar ausschließlich während der einzigen geltenden Evaluierungsperiode, außer wie anderweitig angegeben. Jegliche Nutzung der Software zu anderen Zwecken oder über die geltende Evaluierungsperiode hinaus ist strikt untersagt.

Software für mehrere Umgebungen; Mehrsprachige Software; Dual-Medien-Software; Mehrere Kopien; Softwarebündel. Wenn Sie verschiedene Versionen der Software oder verschiedene Sprachausgaben der Software verwenden, wenn Sie die Software auf mehreren Medien erhalten, wenn Sie anderweitig mehrere Kopien der Software erhalten oder wenn Sie die Software mit einer anderen Software gebündelt erhalten sollten, entspricht die insgesamt zulässige Anzahl Ihrer Computer, auf denen alle Versionen der Software installiert sind, der Anzahl der Lizenzen, die Sie vom Rechtsinhaber bezogen haben, und jede erworbene Lizenz berechtigt Sie zur Installation und Nutzung der Software auf dieser Anzahl von Computern entsprechend den Festlegungen in den Klauseln 2.2 und 2.3, *außer die* Lizenzbedingungen sehen eine anderweitige Regelung vor.

2.2. Wenn die Software auf einem physischen Medium erworben wurde, haben Sie das Recht, die Software auf einer solchen Anzahl von Computern zu verwenden, die auf der Softwareverpackung festgelegt ist.

2.3. Wenn die Software über das Internet erworben wurde, haben Sie das Recht, die Software auf einer solchen Anzahl von Computern zu verwenden, die genannt wurde, als Sie die Lizenz für die Software gekauft haben.

2.4. Sie haben das Recht, eine Kopie der Software anzufertigen, und zwar ausschließlich zu Sicherungszwecken und nur, um die rechtmäßig in Ihrem Besitz befindliche Kopie zu ersetzen, sollte eine solche Kopie verloren gehen, zerstört oder unbrauchbar werden. Diese Sicherungskopie kann nicht zu anderen Zwecken verwendet werden und muss zerstört werden, wenn Sie das Recht verlieren, die Software zu nutzen oder wenn Ihre Lizenz abläuft oder aus irgendeinem Grund im Einklang mit der gültigen Gesetzgebung im Land Ihres Wohnsitzes oder in dem Land, in dem Sie die Software nutzen, gekündigt werden sollte.

2.5. Sie können die nicht-exklusive Lizenz zur Nutzung der Software an andere Personen oder Rechtspersönlichkeiten innerhalb des Rahmens der Ihnen vom Rechtsinhaber gewährten Lizenz übertragen, vorausgesetzt, dass der Empfänger allen Geschäftsbedingungen dieses Vertrags zustimmt bzw. bejaht, Sie vollständig in der vom Rechtsinhaber gewährten Lizenz zu vertreten. In dem Fall, dass Sie die vom Rechtsinhaber gewährten Rechte zur Nutzung der Software vollständig übertragen, müssen Sie alle Kopien der Software, und zwar einschließlich der Sicherungskopie, zerstören. Wenn Sie Empfänger einer übertragenen Lizenz sind, müssen Sie zustimmen, alle Geschäftsbedingungen dieses Vertrags einzuhalten. Wenn Sie den Geschäftsbedingungen dieses Vertrags nicht vollständig zustimmen, dürfen Sie die Software nicht installieren und/oder verwenden. Sie stimmen als Empfänger einer übertragenen Lizenz weiterhin zu, dass Sie über keine zusätzlichen oder besseren Rechte verfügen, als der ursprüngliche Endnutzer, der die Software vom Rechtsinhaber erworben hat.

2.6. Zum Betrieb der Software als Vollversion sollten Sie den Lizenzschlüssel gemäß Beschreibung im Benutzerhandbuch erhalten und installieren.

2.7. Ab dem Zeitpunkt des Übergangs der Software in die Vollversion (mit Ausnahme einer Testversion der Software) haben Sie das Recht, folgende Dienstleistungen entsprechend der Bedingungen unter http://support.kaspersky.com/support/rules zu beziehen:

- Updates der Software über das Internet, wenn und wie der Rechtsinhaber diese auf seiner Webseite oder mittels anderer Online-Dienste veröffentlicht. Jedwede Updates, die Sie erhalten, werden Teil der Software und die Geschäftsbedingungen dieses Vertrags gelten für diese;
- Technische Unterstützung über das Internet sowie technische Unterstützung über die Telefon-Hotline.

3. Wiederholte Aktivierung und Zeitraum für Nutzung der Testversion

3.1. Falls Sie Modifikationen an Ihrem Computer oder an der darauf installierten Software anderer Anbieter vornehmen, kann der Rechtsinhaber von Ihnen verlangen, die Installation des Lizenzschlüssels zu wiederholen.

3.2. Sie haben das Recht, eine Testversion der Software zu nutzen, und zwar gemäß der Festlegung in Klausel 2.1 und ohne jedwede Gebühr für die einzelne geltende Evaluierungsperiode (30 Tage) ab

dem Zeitpunkt der Aktivierung der Software im Einklang mit diesem Vertrag, *und zwar unter der Bedingung, dass* die Testversion Ihnen nicht das Recht auf Updates und technische Unterstützung über das Internet und technische Unterstützung über die Telefon-Hotline einräumt. Wenn der Rechtsinhaber für die einzelne geltende Evaluierungsperiode einen anderen Zeitraum festlegt, erhalten Sie darüber eine Mitteilung.

3.3. Sie haben das Recht, gemäß Klausel 2.1 eine Testversion der Software ohne Gebühr für die zusätzliche einzige geltende Evaluierungsperiode (15 Tage) ab Ende der in Klausel 3.2 erwähnten Software-Testperiode zu nutzen. In diesem Zeitraum ist der Funktionalitätsstatus der Software gemäß Beschreibung im Benutzerhandbuch eingeschränkt.

4. Technische Unterstützung

Die in Klausel 2.7 dieses Vertrags erläuterte technische Unterstützung wird Ihnen gewährt, wenn das neueste Update der Software installiert wird (außer im Fall einer Testversion der Software).
Technischer Support: http://support.kaspersky.com

5. Beschränkungen

5.1. Sie werden die Software nicht emulieren, klonen, vermieten, verleihen, leasen, verkaufen, modifizieren, dekompilieren oder zurückentwickeln oder disassemblieren oder Arbeiten auf Grundlage der Software oder eines Teils davon ableiten, jedoch mit der einzigen Ausnahme eines Ihnen durch geltende Gesetzgebung gewährten Rechts, von dem keine Rücktretung möglich ist, und Sie werden in keiner anderen Form irgendeinen Teil der Software in menschlich lesbare Form umwandeln oder die lizenzierte Software oder irgendeine Teilmenge der lizenzierten Software übertragen, noch irgendeiner Drittpartei gestatten, dies zu tun, außer im Umfang vorangegangener Einschränkungen, die ausdrücklich durch geltendes Recht untersagt sind. Weder Binärcode noch Quellcode der Software dürfen verwendet oder zurückentwickelt werden, um den Programmalgorithmus, der proprietär ist, wiederherzustellen. Alle Rechte, die nicht ausdrücklich hierin gewährt werden, verbleiben beim Rechtsinhaber und/oder dessen Zulieferern, je nachdem, was zutrifft. Jegliche derartige nicht autorisierte Nutzung der Software kann zur sofortigen und automatischen Kündigung dieses Vertrags sowie der hierunter gewährten Lizenz und zu Ihrer straf- und/oder zivilrechtlichen Verfolgung führen.

5.2. Sie werden die Rechte zur Nutzung der Software nicht an eine Drittpartei übertragen, außer entsprechend der Festlegung in Klausel 2.5 dieses Vertrags.

5.3. Sie werden den Aktivierungscode und/oder den Lizenzschlüssel keinen Drittparteien verfügbar machen oder Drittparteien Zugang zum Aktivierungscode und/oder zum Lizenzschlüssel gewähren. Aktivierungscode und/oder Lizenzschlüssel werden/wird als vertrauliche Daten des Rechtsinhabers betrachtet, und Sie werden angemessene Sorgfalt zum Schutz der Vertraulichkeit des Aktivierungscodes und/oder des Lizenzschlüssels walten lassen, sofern Sie den Aktivierungscode und/oder den Lizenzschlüssel entsprechend der Festlegung in Klausel 2.5 dieses Vertrags an Drittparteien übertragen dürfen. Der Rechteinhaber behält sich das Recht vor, jegliche Mittel und Verifizierungsverfahren zu verwenden, um die Gültigkeit der Lizenz bzw. Rechtmäßigkeit einer installierten bzw. auf Ihrem Computer genutzten Kopie der Software zu überprüfen.

5.4. Sie werden die Software nicht an eine Drittpartei vermieten, verleasen oder verleihen.

5.5. Der Rechtsinhaber hat das Recht, den Lizenzschlüssel zu blockieren oder Ihre Lizenz zu kündigen, falls Sie gegen irgendwelche Geschäftsbedingungen dieses Vertrags verstoßen, und zwar ohne irgendeine Rückerstattung an Sie.

5.6. Falls Sie die Testversion der Software verwenden, sind Sie nicht berechtigt, technische Unterstützung, wie in Klausel 4 dieses Vertrags festgelegt, zu erhalten, und Sie sind ebenfalls nicht berechtigt, die Lizenz oder die Rechte zur Nutzung der Software an irgendeine Drittpartei zu übertragen.

5.7. Ohne Beeinträchtigung anderer möglicher Rechtsbehelfe aufgrund des Gesetzes oder Billigkeitsrechts des Rechteinhabers, hat der Rechteinhaber im Fall eines Verstoßes gegen irgendeine der Bedingungen dieses Vertrags durch Sie jederzeit das Recht, die Lizenz zur Nutzung dieser Software, ohne Mitteilung an Sie und ohne Erstattung des vollständigen oder anteiligen Kaufpreises zu beenden.

6. Eingeschränkte Garantie und Haftungsausschluss

6.1. Der Rechtsinhaber garantiert, dass die Software im Wesentlichen im Einklang mit den im Nutzerhandbuch dargelegten Spezifikationen und Beschreibungen funktionieren wird, jedoch vorausgesetzt, dass eine solche eingeschränkte Garantie nicht für Folgendes gilt: (w) Mängel Ihres Computers und zugehörigen Verstoß, wofür der Rechtsinhaber ausdrücklich jedwede Gewährleistungsverantwortung ablehnt; (x) Funktionsstörungen, Defekte oder Ausfälle, resultierend aus falscher Verwendung, Missbrauch, Unfall, Nachlässigkeit, unsachgemäßer/m Installation, Betrieb oder Wartung, Diebstahl, Vandalismus, höherer Gewalt, terroristischen Akten, Stromausfällen oder -schwankungen, Unglück, Veränderung, nicht zulässiger Modifikation oder Reparaturen durch eine Partei außer dem Rechtsinhaber oder Maßnahmen einer sonstigen Drittpartei oder Aktionen ihrerseits, oder Ursachen außerhalb der Kontrolle des Rechtsinhabers; (y) jedweder Defekt, der dem Rechtsinhaber nicht durch Sie bekannt gemacht wird, sobald dies nach dem ersten Auftreten des Defekts möglich ist; und (z) Inkompatibilität, verursacht durch Hardware- und/oder Software-Komponenten, die auf Ihrem Computer installiert sind.

6.2. Sie bestätigen, akzeptieren und erkennen an, dass keine Software frei von Fehlern ist, und Sie sind angehalten, den Computer mit einer für Sie geeigneten Häufigkeit und Beständigkeit zu sichern.

6.3. Der Rechtsinhaber gibt keine Garantie, dass die Software im Fall von Verstößen gegen die Bedingungen, wie im Nutzerhandbuch oder in diesem Vertrag beschrieben, einwandfrei funktionieren wird.

6.4. DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND DER RECHTSINHABER GIBT KEINE ZUSICHERUNG UND KEINE GEWÄHRLEISTUNG IN BEZUG AUF IHRE NUTZUNG ODER LEISTUNG. DER RECHTSINHABER UND SEINE PARTNER GEWÄHREN AUßER DEN GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN, DIE DURCH GELTENDES RECHT NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KÖNNEN, KEINE GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN (AUSDRÜCKLICHER ODER STILLSCHWEIGENDER NATUR, DIE ENTWEDER AUS EINER GESCHÄFTSBEZIEHUNG ODER EINEM HANDELSBRAUCH ENTSTEHEN BZW. AUS GESETZLICHEN, GEWOHNHEITSRECHTLICHTEN ODER ANDEREN VORSCHRIFTEN ABGELEITET WERDEN) HINSICHTLICH JEDWEDER ANGELEGENHEIT, EINSCHLIEßLICH (OHNE EINSCHRÄNKUNG) VON NICHTVERLETZUNG VON RECHTEN DRITTER, MARKTGÄNGIGKEIT, BEFRIEDIGENDE QUALITÄT, INTEGRIERUNG ODER BRAUCHBARKEIT FÜR EINEN BESTIMMTEN ZWECK. SIE TRAGEN DAS GESAMTE STÖRUNGSRISIKO UND DAS GESAMTRISIKO HINSICHTLICH DER LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, UM IHRE VORGESEHENEN RESULTATE ZU ERZIELEN, UND FÜR DIE INSTALLATION SOWIE DIE NUTZUNG DER SOFTWARE UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORANGEGANGENEN BESTIMMUNGEN MACHT DER RECHTSINHABER KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNG, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON UNTERBRECHUNGEN ODER SONSTIGEN STÖRUNGEN IST ODER DASS DIE SOFTWARE JEDWEDE ODER ALL IHRE ANFORDERUNGEN ERFÜLLEN WIRD, UNGEACHTET DESSEN, OB GEGENÜBER DEM RECHTSINHABER OFFEN GELEGT ODER NICHT.

7. <u>Haftungsausschluss und Haftungsbeschränkungen</u>

INSOWEIT GESETZLICH STATTHAFT, SIND DER RECHTSINHABER UND SEINE PARTNER UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE SPEZIELLEN ODER BEILÄUFIGEN SCHÄDEN, STRAFZUSCHLAG ZUM SCHADENERSATZ, INDIREKTE ODER FOLGESCHÄDEN (EINSCHLIEßLICH UND NICHT BESCHRÄNKT AUF SCHÄDEN AUS VERLUST VON GEWINN ODER VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSUNTERBRECHUNG, FÜR VERLUST VON PRIVATSPHÄRE, KORRUPTION, BESCHÄDIGUNG UND VERLUST VON DATEN ODER PROGRAMMEN, FÜR VERSÄUMNIS EINER PFLICHTERFÜLLUNG, EINSCHLIEßLICH JEDWEDER GESETZLICHER PFLICHTEN, TREUEPFLICHT ODER PFLICHT ZUR WAHRUNG ANGEMESSENER SORGFALT, FÜR NACHLÄSSIGKEIT, FÜR WIRTSCHAFTLICHEN VERLUST UND FÜR FINANZIELLEN ODER JEDWEDEN SONSTIGEN VERLUST), DIE AUS ODER AUF IRGENDEINE WEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE, DER BEREITSTELLUNG ODER DEM VERSÄUMNIS DER BEREITSTELLUNG TECHNISCHER UNTERSTÜTZUNG ODER SONSTIGER DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND ZUGEHÖRIGEM INHALT MITTELS DER SOFTWARE RESULTIEREN, ODER SICH ANDERWEITIG AUS DER NUTZUNG DER SOFTWARE ODER ANDERWEITIG UNTER BZW. IM ZUSAMMENHANG MIT EINER BESTIMMUNG DIESES VERTRAGS ERGEBEN, ODER DIE FOLGE EINES VERTRAGSBRUCHS ODER UNERLAUBTER HANDLUNG

(EINSCHLIEßLICH NACHLÄSSIGKEIT, FALSCHANGABE, JEDWEDER STRIKTEN HAFTUNGSVERPFLICHTUNG ODER -PFLICHT), ODER EINER VERLETZUNG GESETZLICHER PFLICHTEN ODER DER GEWÄHRLEISTUNG DES RECHTSINHABERS ODER EINES SEINER PARTNER SIND, UND ZWAR AUCH DANN NICHT, WENN DER RECHTSINHABER ODER EINER SEINER PARTNER BEZÜGLICH DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.

SIE STIMMEN ZU, DASS IN DEM FALL, DASS DER RECHTSINHABER UND/ODER SEINE PARTNER HAFTBAR GEMACHT WERDEN/WIRD, DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER AUF DIE KOSTEN DER SOFTWARE BESCHRÄNKT IST. UNTER KEINEN UMSTÄNDEN WIRD DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE ERSTATTETEN KOSTEN AN DEN RECHTSINHABER ODER DEN PARTNER ÜBERSTEIGEN (JE NACHDEM, WAS ZUTRIFFT).

NICHTS IN DIESEM VERTRAG SCHLIEßT EINEN ANSPRUCH AUFGRUND VON TOD UND PERSONENSCHADEN AUS ODER SCHRÄNKT DIESEN EIN. IN DEM FALL, DASS EIN HAFTUNGSAUSSCHLUSS, EIN AUSSCHLUSS ODER EINE EINSCHRÄNKUNG IN DIESEM VERTRAG AUFGRUND GELTENDEN RECHTS NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN, WIRD NUR EIN SOLCHER HAFTUNGSAUSSCHLUSS, AUSSCHLUSS ODER EINE EINSCHRÄNKUNG NICHT FÜR SIE GELTEN, UND SIE SIND WEITERHIN AN JEDWEDE VERBLEIBENDEN HAFTUNGSAUSSCHLÜSSE, AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN GEBUNDEN.

8. <u>GNU und sonstige Drittpartei-Lizenzen</u>

Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software“). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert. Falls irgendwelche Open Source Software-Lizenzen es erforderlich machen, dass der Rechtsinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms bereitstellt, welche umfassender sind, als die in diesem Vertrag gewährten Rechte, dann werden derartige Rechte Vorrang vor den hierin festgelegten Rechten und Einschränkungen haben.

9. <u>Geistiges Eigentum</u>

9.1 Sie stimmen zu, dass die Software sowie die Urheberschaft, Systeme, Ideen, Betriebsmethoden, Dokumentation und sonstige in der Software enthaltenen Informationen proprietäres geistiges Eigentum und/oder die wertvollen Geschäftsgeheimnisse des Rechtsinhabers oder seiner Partner sind und dass der Rechtsinhaber und seine Partner, je nachdem was zutrifft, durch das Zivil- und Strafrecht sowie durch Gesetze zum Urheberrecht, bezüglich Geschäftsgeheimnissen, Handelsmarken und Patenten der Russischen Föderation, der Europäischen Union und der Vereinigten Staaten sowie anderer Länder und internationaler Übereinkommen geschützt sind. Dieser Vertrag gewährt Ihnen keinerlei Rechte am geistigen Eigentum, einschließlich an jeglichen Handelsmarken und Servicemarken des Rechtsinhabers und/oder seiner Partner („Handelsmarken“). Sie dürfen die Handelsmarken nur so weit nutzen, um von der Software im Einklang mit der akzeptierten Handelsmarkenpraxis erstellte Druckausgaben zu identifizieren, einschließlich der Identifizierung des Namens des Besitzers der Handelsmarke. Eine solche Nutzung der Handelsmarke gibt Ihnen keinerlei Besitzrechte an dieser Handelsmarke. Der Rechtsinhaber und/oder seine Partner besitzen und behalten alle Rechte, Titel und Anteile an der Software, einschließlich (ohne jedwede Einschränkung) jedweden Fehlerkorrekturen, Erweiterungen, Updates oder sonstigen Modifikationen an der Software, ob durch den Rechtsinhaber oder eine beliebige Drittpartei vorgenommen, und allen Urheberrechten, Patenten, Rechten an Geschäftsgeheimnissen, Handelsmarken und sonstigem geistigen Eigentum daran. Ihr Besitz, die Installation oder Nutzung der Software lässt den Titel am geistigen Eigentum an der Software nicht auf Sie übergehen, und Sie erwerben keinerlei Rechte an der Software, außer jene ausdrücklich in diesem Vertrag dargelegten. Alle hierunter erstellten Kopien der Software müssen dieselben proprietären Informationen enthalten, die auf und in der Software erscheinen. Mit Ausnahme der hierin

aufgeführten Bestimmungen gewährt Ihnen dieser Vertrag keine Rechte geistigen Eigentums an der Software und Sie bestätigen, dass diese unter diesem Vertrag gewährte Lizenz Ihnen gemäß den weiteren Festlegungen hierin ausschließlich das Recht auf eingeschränkte Nutzung unter den Geschäftsbedingungen dieses Vertrags gewährt. Der Rechtsinhaber behält sich alle Rechte vor, die Ihnen nicht ausdrücklich in diesem Vertrag gewährt wurden.

9.2 Sie bestätigen, dass der Quellcode, der Aktivierungscode und/oder den Lizenzschlüssel für die Software Eigentum des Rechtsinhabers sind und Geschäftsgeheimnisse des Rechtsinhabers konstituieren. Sie stimmen zu, den Quellcode der Software nicht zu modifizieren, abzuwandeln, zu übersetzen, zurückzuentwickeln, zu dekompilieren oder auf sonstige Weise zu versuchen, den Quellcode ausfindig zu machen.

9.3 Sie stimmen zu, die Software in keinster Weise zu modifizieren oder abzuändern. Sie dürfen die Urheberrechtshinweise oder sonstige proprietäre Hinweise auf jedweden Kopien der Software nicht entfernen oder verändern.

10. Geltendes Recht; Schiedsverfahren

Dieser Vertrag unterliegt den Gesetzen der Russischen Föderation und wird nach diesen ausgelegt, und zwar ohne Bezug auf gegenteilige gesetzliche Regelungen und Prinzipien. Dieser Vertrag wird nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf unterliegen, dessen Anwendung ausschließlich ausgeschlossen wird. Jede Meinungsverschiedenheit, die aus den Bedingungen dieses Vertrags, deren Auslegung oder Anwendung oder einem Verstoß gegen diese resultiert, wird, außer falls durch unmittelbare Verhandlung beigelegt, durch das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation in Moskau, in der Russischen Föderation, beigelegt. Jeder vom Schlichter abgegebene Schiedsspruch ist für die beteiligten Parteien endgültig und bindend und jedwedes Urteil bezüglich eines solchen Schiedsspruchs kann von jedem Gericht der zuständigen Jurisdiktion durchgesetzt werden. Nichts in diesem Abschnitt 11 wird eine Partei daran hindern, von einem Gericht der zuständigen Jurisdiktion rechtmäßige Entschädigung zu verlangen oder zu erhalten, sei es vor, während oder nach einem Schiedsverfahren.

11. Zeitraum für Rechtsverfolgung.

Von den Parteien dieses Vertrags kann keine Rechtsverfolgung, ungeachtet der Form, die sich aus Transaktionen unter diesem Vertrag ergibt, nach mehr als einem (1) Jahr nach dem Eintreten des Klagegrundes oder der Entdeckung dessen Eintritts ergriffen werden, außer, dass eine Rechtsverfolgung für Verletzung von Rechten geistigen Eigentums innerhalb des maximal geltenden gesetzlichen Zeitraums ergriffen wird.

12. Vollständigkeit der Vereinbarung, Salvatorische Klausel, kein Verzicht.

Dieser Vertrag stellt die Gesamtvereinbarung zwischen Ihnen und dem Rechtsinhaber dar und ersetzt jegliche sonstigen, vorherigen Vereinbarungen, Vorschläge, Kommunikation oder Ankündigung, ob mündlich oder schriftlich, in Bezug auf die Software oder den Gegenstand dieser Vereinbarung. Sie bestätigen, dass Sie diesen Vertrag gelesen haben, ihn verstehen und seinen Bedingungen zustimmen. Falls eine Bestimmung dieses Vertrags von einem Gericht der zuständigen Jurisdiktion insgesamt oder in Teilen als untauglich, ungültig oder aus welchen Gründen auch immer als nicht durchsetzbar angesehen wird, wird diese Bestimmung enger ausgelegt, damit sie rechtmäßig und durchsetzbar wird, und der Gesamtvertrag wird an diesem Umstand nicht scheitern, und die Ausgewogenheit des Vertrags bleibt weiterhin vollinhaltlich gültig und wirksam, so weit gesetzlich oder nach Billigkeitsrecht zulässig, während der ursprüngliche Inhalt weitest möglich beibehalten wird. Kein Verzicht auf eine hierin enthaltene Bestimmung oder Kondition ist gültig, außer in schriftlicher Form und durch Sie und einen autorisierten Vertreter des Rechtsinhabers unterzeichnet, vorausgesetzt, dass kein Verzicht einer Verletzung einer Bestimmung dieses Vertrags einen Verzicht eines vorherigen, gleichzeitigen oder Folgeverstoßes konstituiert. Nichtverfolgung oder fehlende Durchsetzung einer Bestimmung dieses Vertrags durch den Rechtsinhaber kann nicht als Verzicht auf diese Bestimmung oder dieses Recht geltend gemacht werden.

13. Kontaktinformationen des Rechteinhabers

Sollten Sie Fragen in Bezug auf diesen Vertrag haben oder sollten Sie wünschen, sich aus irgendeinem Grund mit dem Rechtsinhaber in Verbindung zu setzen, kontaktieren Sie bitte unsere Kundendienstabteilung unter:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moskau, 123060
Russische Föderation
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-Mail: info@kaspersky.com
Webseite: www.kaspersky.com

ÜBER DIESES HANDBUCH

Dieses Handbuch informiert über Installation, Konfiguration und Verwendung des Programms Kaspersky Password Manager. Das Dokument ist für Heimanwender gedacht. Zur Verwendung des Programms sind Grundkenntnisse im Umgang mit einem PC erforderlich: Der Anwender sollte die Oberfläche und die Funktionen des Betriebssystems Microsoft Windows auf grundlegendem Niveau beherrschen sowie gängige E-Mail-Programme und Browser wie Microsoft Office Outlook und Microsoft Internet Explorer bedienen können.

Das Dokument soll:

- dem Nutzer helfen, das Programm zu aktivieren und unter Berücksichtigung individueller Aufgaben optimal anzupassen.
- Fragen, die sich auf das Programm beziehen, schnell beantworten.
- auf alternative Informationsquellen über das Programm und auf Möglichkeiten des technischen Supports hinweisen.

IN DIESEM ABSCHNITT

IN DIESEM DOKUMENT

Das Benutzerhandbuch für Kaspersky Password Manager besteht aus folgenden Kapiteln:

Zusätzliche Informationsquellen

Dieser Abschnitt enthält eine Beschreibung der Quellen, die zusätzliche Informationen über das Programm bieten, und verweist auf Internetressourcen, die zur Diskussion über das Programm, für Vorschläge, sowie für Fragen und Antworten dienen.

Kaspersky Password Manager

Dieser Abschnitt enthält eine Beschreibung der Möglichkeiten der Anwendung sowie über seine Komponenten und Grundfunktionen.

Programm aktivieren

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmlizenzierung zusammenhängen und enthält eine Anleitung zur Programmaktivierung.

Oberfläche des Kaspersky Password Manager

Dieser Abschnitt beschreibt die wichtigsten Elemente der grafischen Programmoberfläche.

Kennwort-Datenbank verwalten

Dieser Abschnitt informiert darüber, wie Daten erstellt und verwendet werden, die für das automatische Ausfüllen von Formularen auf Webseiten und in Programmen dienen.

Programmeinstellungen anpassen

Dieser Abschnitt informiert darüber, wie das Programm für eine möglichst effektive Arbeit angepasst werden kann.

Erstellen von sicheren Kennwörtern

Dieser Abschnitt informiert über die Verwendung des Generators für sichere Kennwörter.

Verwendung einer portablen Version des Kaspersky Password Managers

Dieser Abschnitt informiert darüber, wie eine portable Version von Kaspersky Password Manager erstellt und verwendet wird.

FORMATIERUNG MIT BESONDERER BEDEUTUNG

Die Bedeutung der in diesem Dokument verwendeten Textformatierungen wird in folgender Tabelle erläutert.

Tabelle 1. Formatierung mit besonderer Bedeutung

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Beachten Sie, dass ...	Warnungen sind rot geschrieben und eingerahmt. Warnungen enthalten wichtige Informationen, die z.B. auf Aktionen hinweisen, die im Hinblick auf die Computersicherheit als kritisch gelten.
Es wird empfohlen,...	Hinweise sind eingerahmt. Hinweise enthalten hilfreiche und informative Angaben.
Beispiel: ...	Beispiele sind gelb unterlegt und mit "Beispiel" überschrieben.
Das *Update* ist...	Neue Begriffe sind kursiv geschrieben.
ALT+F4	Bezeichnungen von Tasten sind halbfett und in Großbuchstaben geschrieben. Tastenbezeichnungen, die mit einem Pluszeichen verbunden sind, bedeuten eine Tastenkombination.
Aktivieren	Die Namen von Elementen der Benutzeroberfläche (z.B. Eingabefelder, Menübefehle, Schaltflächen) sind halbfett geschrieben.
Gehen Sie folgendermaßen vor, um den Aufgabenzeitplan anzupassen:	Der erste Satz einer Anleitung ist kursiv geschrieben.
`help`	Texte in der Befehlszeile oder Meldungstexte, die das Programm auf dem Bildschirm anzeigt, werden durch spezielle Schrift hervorgehoben.
<IP-Adresse Ihres Computers>	Variable stehen in eckigen Klammern. Eine Variable muss in einem konkreten Fall durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.

ZUSÄTZLICHE INFORMATIONSQUELLEN

Fragen zu Auswahl, Kauf, Installation oder Verwendung von Kaspersky Password Manager, lassen sich unter Verwendung unterschiedlicher Informationsquellen beantworten. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

IN DIESEM ABSCHNITT

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Kaspersky Lab bietet folgende Informationsquellen zu dem Programm an:

- Seite über das Programm auf der Webseite von Kaspersky Lab
- Seite über das Programm auf der Webseite des Technischen Supports (in der Wissensdatenbank)
- Seite des Interaktiven Supports
- Elektronisches Hilfesystem

Seite auf der Webseite von Kaspersky Lab

Auf dieser Seite (http://www.kaspersky.com/de/kaspersky-password-manager) finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

Auf dieser Seite (http://support.kaspersky.com/de/kpm) finden Sie Artikel, die von Spezialisten des technischen Supports veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung vom Programm. Sie sind nach Themen wie "Mit der Produktlizenz arbeiten", "Update anpassen" oder "Störungen bei der Arbeit beheben" angeordnet. Die Artikel können auch Fragen behandeln, die neben diesem Programm auch andere Produkte von Kaspersky Lab betreffen. Außerdem können sie allgemeine Neuigkeiten über den Technischen Support enthalten.

Interaktiver Support

Auf der Seite dieses Dienstes finden Sie eine regelmäßig aktualisierte Datenbank mit häufig auftretenden Fragen und Antworten über die Arbeit des Programms. Um diesen Dienst nutzen zu können, ist eine Internetverbindung erforderlich.

- Um zur Serviceseite zu wechseln, klicken Sie mit der rechten Maustaste auf das Programmsymbol in der Taskleiste und gehen Sie auf "**Hilfe**" - "**Technischer Support**".

Elektronisches Hilfesystem

Im Lieferumfang des Programms ist eine vollständige und kontextorientierte Hilfedatei enthalten. Sie bietet Informationen zu folgenden Aspekten der Verwaltung des Computerschutzes: Anzeige des Schutzstatus, Untersuchung bestimmter Computerbereiche auf Viren, Ausführen anderer Aufgaben. Außerdem bietet die vollständige und kontextorientierte Hilfedatei Informationen zu jedem Programmfenster: verfügbare Einstellungen und deren Beschreibung sowie eine Liste mit den auszuführenden Aufgaben.

Um die Hilfe zu öffnen, klicken Sie im entsprechenden Fenster auf die Schaltfläche **Hilfe** oder auf die Taste **F1**.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse http://forum.kaspersky.com diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf von der Kaspersky Produkte sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung in Deutschland über unser Kontaktformular unter http://www.kasperskylab.de/kontakt/ zur Verfügung.

KASPERSKY PASSWORD MANAGER

Kaspersky Password Manager speichert und schützt alle Ihre persönlichen Daten (z.B. Kennwörter, Benutzernamen, Nummern für Instant Messenger, Kontaktdaten, Telefonnummern usw.). Kaspersky Password Manager verknüpft Kennwörter und Benutzerkonten mit Programmen von Microsoft Windows oder mit Webseiten, für die sie verwendet werden. Alle Informationen werden in verschlüsselter Form in einer Kennwort-Datenbank gespeichert, auf die der Zugriff nur mit einem Master-Kennwort möglich ist. Persönliche Daten sind leicht zugänglich, wenn die Kennwort-Datenbank nicht blockiert ist. Nach dem Start einer Webseite oder eines Programms fügt Kaspersky Password Manager automatisch das Kennwort, den Benutzernamen und andere persönliche Daten ein. Somit ist es ausreichend, sich nur ein einzelnes Kennwort zu merken.

In der Grundeinstellung wird Kaspersky Password Manager automatisch beim Hochfahren des Betriebssystems gestartet. Die Komponente wird in Programme integriert, wodurch erlaubt wird, persönliche Daten direkt aus einem Programmfenster zu verwalten.

Kaspersky Password Manager verfolgt die Aktionen, die Programme mit Kennwörtern ausführen, und verhindert das Abfangen und den Diebstahl persönlicher Informationen. Die Komponente untersucht Programme, die Kennwörter verwenden oder von anderen Programmen ein Kennwort abfragen, und bietet Ihnen anschließend an, eine verdächtige Aktion zu erlauben oder zu verbieten.

Außerdem bietet Kaspersky Password Manager folgende Möglichkeiten:

- Speicherung und Verwendung Ihrer Kennwörter (s. S. 31)
- Suche nach Benutzerkonten, Kennwörtern, Benutzernamen und anderen persönlichen Informationen in der Kennwort-Datenbank (s. S. 32)
- Generieren von zuverlässigen Kennwörtern (s. S. 50), wenn neue Benutzerkonten eingerichtet werden.
- Speicherung aller Kennwörter auf einem Wechseldatenträger (s. S. 51).
- Wiederherstellung der Kennwort-Datenbank aus einer Sicherungskopie (s. S. 34).
- Schutz der Kennwörter vor unerlaubtem Zugriff (s. S. 22).

PROGRAMM AKTIVIEREN

Das Programm wird durch das Registrieren eines Lizenzschlüssels aktiviert. Auf Basis des Lizenzschlüssels wird ermittelt, ob eine Nutzungsberechtigung für die aktuelle Programmversion vorliegt.

Jeder Programmversion entspricht ein spezieller Lizenzschlüssel, der aus einer Zeichenfolge besteht. Wenn Sie Kaspersky Password Manager kaufen, wird Ihnen der Lizenzschlüssel per E-Mail zugeschickt.

Der Lizenzschlüssel ist für die aktuelle Programmversion und für alle Updates des Programms gültig.

Stellen Sie vor der Installation von Programm-Upgrades sicher, dass Sie den Lizenzschlüssel gespeichert haben.

Kaspersky Password Manager arbeitet ab der Installation für 30 Tage im vollfunktionalen Modus. Nach Ablauf der Testversion werden einige Programmfunktionen deaktiviert. Eine Lizenz kann entweder während der ersten Konfiguration von Kaspersky Password Manager im Fenster des Konfigurationsassistenten (s. S. 37) oder während der 30-tägigen Testphase aktiviert werden. Wenn Sie noch keine Programmlizenz erworben haben, können Sie im Verlauf der Programmaktivierung eine Lizenz kaufen.

Der Kauf einer Lizenz für Kaspersky Password Manager ist auch auf folgende Weise möglich:

- im Online-Shop von Kaspersky Lab.
- aus dem Kontextmenü von Kaspersky Password Manager – Wählen Sie dazu im Kontextmenü des Programms den Punkt **Lizenz kaufen** aus.
- im Fenster mit Informationen über das Programm – Wählen Sie dazu im Kontextmenü des Programms den Punkt **Hilfe** –> **Über Kaspersky Password Manager** aus.
- Wenn die Kennwort-Datenbank mit Hilfe des Master-Kennworts freigegeben wird – Verwenden Sie dazu im Freigabefenster den Link **Lizenzschlüssel online kaufen**.
- mit der Titelleisten-Schaltfläche – Wählen Sie dazu im Menü der Titelleisten-Schaltfläche den Punkt **Aktivierung** aus.

Das Programm kann auf folgende Weise aktiviert werden:

- Aus dem Kontextmenü des Programms. Wählen Sie dazu im Kontextmenü des Programms den Punkt **Hilfe** –> **Aktivierungscode angeben** aus.
- Im Fenster mit Informationen über das Programm. Wählen Sie dazu im Kontextmenü des Programms den Punkt **Hilfe** –> **Über Kaspersky Password Manager**.
- Wenn die Kennwort-Datenbank mit Hilfe des Master-Kennworts freigegeben wird. Verwenden Sie dazu im Freigabefenster den Link **Lizenzschlüssel angeben, um eine kommerzielle Version zu aktivieren**.

Gehen Sie folgendermaßen vor, um das Programm zu aktivieren:

1. Wählen Sie im Kontextmenü von Kaspersky Password Manager den Punkt **Hilfe** –> **Aktivierungscode angeben**.
2. Wechseln Sie bei Bedarf im folgenden Fenster zum Kauf einer Lizenz. Klicken Sie dazu auf den Link **Online kaufen**. Geben Sie nach dem Kauf einer Lizenz den Lizenzschlüssel an und bestätigen Sie die Eingabe.

OBERFLÄCHE DES KASPERSKY PASSWORD MANAGER

In diesem Kapitel werden die Grundprinzipien der Arbeit mit Kaspersky Password Manager ausführlich beschrieben.

IN DIESEM ABSCHNITT

SYMBOL IM INFOBEREICH DER TASKLEISTE

Sofort nach dem Start von Kaspersky Password Manager erscheint sein Symbol im Infobereich der Taskleiste von Microsoft Windows.

In Abhängigkeit von der Situation besitzt das Symbol von Kaspersky Password Manager folgendes Aussehen:

- aktiv (grün) – Kaspersky Password Manager ist freigegeben. Der Zugriff auf persönliche Daten ist erlaubt.
- inaktiv (rot) – Kaspersky Password Manager ist blockiert. Die persönlichen Daten sind nicht verfügbar.

Durch Klick auf das Symbol werden folgende Oberflächenelemente verfügbar:

- Kontextmenü (s. S. 18).
- Zeiger von Kaspersky Password Manager.

KONTEXTMENÜ VON KASPERSKY PASSWORD MANAGER

Das Kontextmenü des Kaspersky Password Managers bietet Zugriff auf die wichtigsten Schutzaufgaben und enthält folgende Punkte:

- **Blockieren / Freigeben** – Verbot / Erlaubnis des Zugriffs auf Ihre persönlichen Daten.
- **Benutzerkonten** – schneller Zugriff auf häufig verwendete Benutzerkonten. Die Anzahl der Benutzerkonten in der Kennwort-Datenbank wird in Klammern genannt. Eine Liste der häufig verwendeten Benutzerkonten wird automatisch angelegt. Die Liste ist vorhanden, wenn festgelegt wurde, dass sie im Kontextmenü angezeigt werden soll (s. S. 38). Beim ersten Programmstart fehlt die Liste, weil noch kein Eintrag verwendet wurde.

- **Persönliche Notizen** – schneller Zugriff auf persönliche Notizen. Die Anzahl der persönlichen Notizen in der Kennwort-Datenbank wird in Klammern genannt.
- **Hinzufügen** – Hinzufügen eines neuen Benutzerkontos, einer persönlichen Notiz oder einer Visitenkarte.
- **Password Manager** – Öffnen des Programmhauptfensters (s. S. 19).
- **Einstellungen** – Anpassen der Programmparameter.
- **Portable Version** - Assistent zum Erstellen einer portablen Version des Programms starten (s. S. 51).
- **Kennwort-Generator** – sichere Kennwörter erstellen (s. S. 50).
- **Hilfe** – Hilfesystem für das Programm öffnen.
- **Beenden** – Arbeit des Programms beenden (bei Auswahl dieses Menüpunkts wird das Programm aus dem Arbeitsspeicher des Computers entfernt).

Wenn das Programm nicht freigegeben ist, wird der Zugriff auf Ihre persönlichen Daten verboten. In diesem Fall stehen im Kontextmenü nur folgende Punkte zur Verfügung: **Freigeben**, **Kennwort-Generator**, **Hilfe** und **Beenden**.

➡ *Um das Kontextmenü zu öffnen,*

zeigen Sie im Infobereich der Taskleiste mit der Maus auf das Symbol des Kaspersky Password Managers und führen Sie einen Rechtsklick aus.

FENSTER VON KASPERSKY PASSWORD MANAGER

Das Fenster **Kaspersky Password Manager** besteht aus drei Teilen:

- Schaltfläche zum Blockieren / Entsperren der Kennwort-Datenbank (s. S. 22).
- Schaltflächen für den schnellen Zugriff auf die wichtigsten Funktionen des Kaspersky Password Managers: Kennwort erstellen, Visitenkarte erstellen, Kennwort-Datenbank verwalten, Einstellungen für die Arbeit, das Erstellen und die Synchronisierung einer portablen Version des Kaspersky Password Managers anpassen (nicht verfügbar, wenn die Kennwort-Datenbank blockiert ist).
- Schaltfläche des Kennwort-Generators (s. S. 50).

Außerdem stehen folgende Schaltflächen und Links zur Verfügung:

- **Hilfe** - Hilfesystem des Kaspersky Password Managers öffnen.
- **Zurück** - in das Hauptfenster von Kaspersky Password Manager wechseln.

FENSTER DER KENNWORT-DATENBANK

Das Fenster der Kennwort-Datenbank besteht aus drei Teilen:

- Im oberen Fensterbereich können Funktionen von Kaspersky Password Manager ausgewählt und wichtige Aufgaben ausgeführt werden.
- Der mittlere Bereich des Fensters enthält eine Liste aller Benutzerkonten und anderen persönlichen Daten. Außerdem dient er der Verwaltung von persönlichen Informationen.
- Im unteren Fensterbereich befinden sich Links zur Verwaltung der Kennwort-Datenbank.

Außerdem können Sie die Suchzeile im oberen Fensterbereich verwenden. Mit der Suchzeile kann in der Kennwort-Datenbank mit Hilfe eines Schlüsselworts nach bestimmten Informationen gesucht werden.

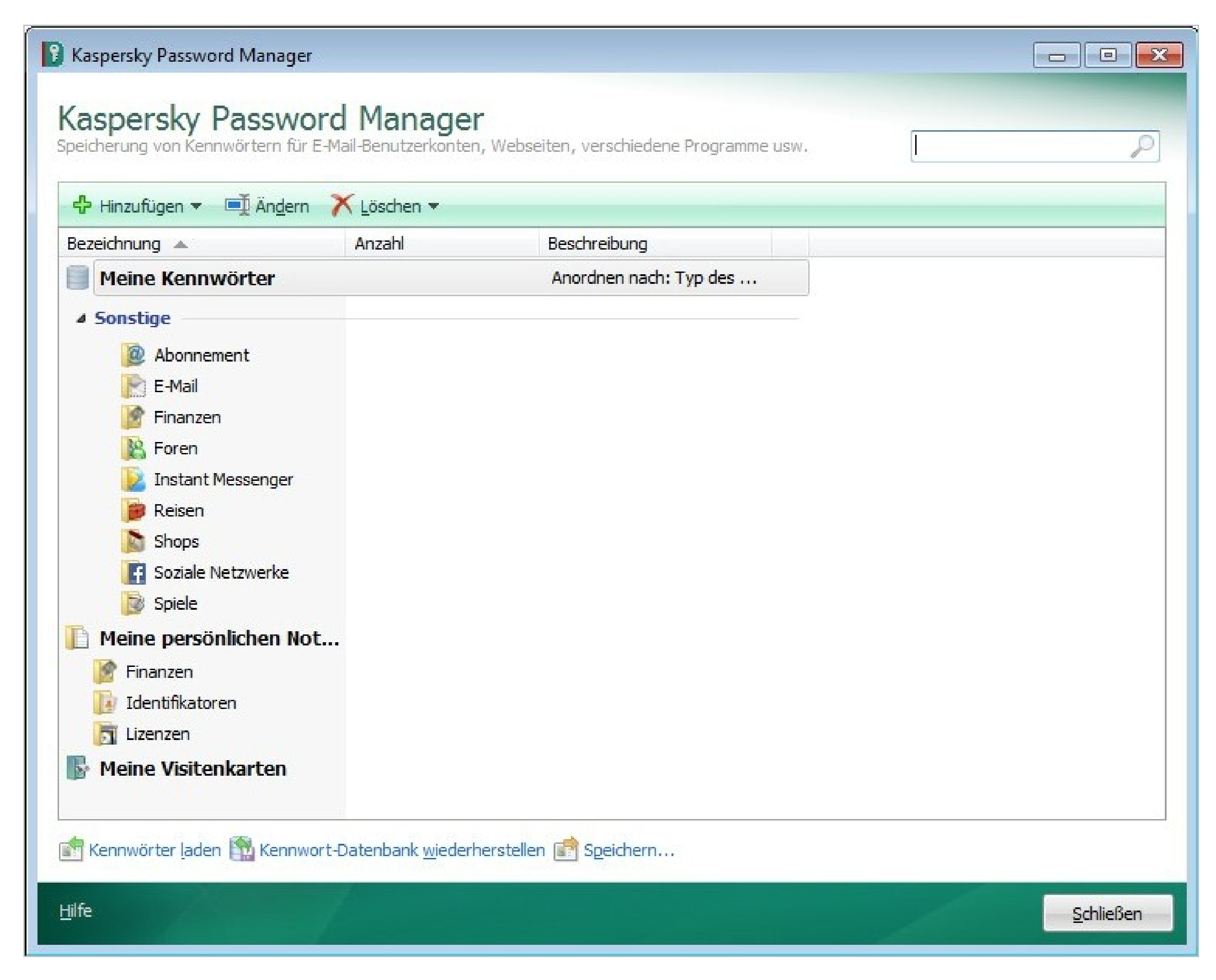


Abbildung 1. Fenster der Kennwort-Datenbank

KONFIGURATIONSFENSTER

Das Konfigurationsfenster von Kaspersky Password Manager kann auf eine der folgenden Arten geöffnet werden:

- aus dem Kontextmenü von Kaspersky Password Manager (s. S. 18) – Wählen Sie dazu im Kontextmenü von Kaspersky Password Manager den Punkt **Einstellungen**.
- aus dem Fenster von Kaspersky Password Manager **–** Klicken Sie dazu auf **Einstellungen**.

Das Konfigurationsfenster besteht aus zwei Teilen:

- Im linken Bereich des Fensters befindet sich eine Liste der Programmfunktionen.
- Auf der rechten Seite des Fensters steht eine Liste der Einstellungen für die ausgewählte Funktion, Aufgabe usw. zur Verfügung.

TITELLEISTEN-SCHALTFLÄCHE

Die Titelleisten-Schaltfläche erlaubt die Arbeit mit Ihren persönlichen Daten aus einem Programmfenster / einer Webseite. Die Schaltfläche befindet sich in der oberen rechten Ecke eines Programms.

Durch Klick auf die Titelleisten-Schaltfläche wird ein Menü mit der Liste der Benutzernamen geöffnet, die mit diesem Programm / mit dieser Webseite verknüpft sind. Bei Auswahl eines Benutzernamens füllt Kaspersky Password Manager auf Grundlage der Daten aus der Kennwort-Datenbank automatisch die Authentifizierungsfelder aus.

Die Titelleisten-Schaltfläche ist aktiv , wenn der Kaspersky Password Manager nicht blockiert ist (s. S. 22). Durch Klick auf die Schaltfläche gelangt man zu folgenden Aktionen:

- **Benutzerkonto hinzufügen** – Hinzufügen eines neuen Benutzerkontos.
- **Benutzerkonto ändern** – Hinzufügen eines Benutzernamens / Ändern eines aktivierten Benutzerkontos. Der Menüpunkt ist vorhanden, wenn das Benutzerkonto aktiviert wurde.
- **Internet-Benutzerkonten** – Anzeige einer Liste aller Benutzerkonten für das Internet und Start eines dieser Benutzerkonten. Die Anzahl der Benutzerkonten in der Kennwort-Datenbank wird in Klammern genannt.
- Liste der häufig verwendeten Benutzerkonten – Start eines Benutzerkontos aus der Liste. Die Liste wird aufgrund der Verwendungshäufigkeit von Benutzerkonten automatisch angelegt. Die Liste ist im Menü vorhanden, wenn zusätzlich ihre Anzeige angepasst wurde (s. S. 38).
- **Visitenkarten** – Anzeige einer Liste der erstellten Visitenkarten und Auswahl einer Visitenkarte für ein Anmeldeformular.
- **Hilfe** – Hilfe für das Programm.

Die Titelleisten-Schaltfläche ist aktiv , wenn Kaspersky Password Manager nicht blockiert ist. In diesem Fall ist es nicht möglich, durch Klick auf diese Schaltfläche zu dem genannten Aktionen zu gelangen. Die inaktive Schaltfläche wird in einem Programmfenster angezeigt, wenn zusätzlich die Einstellungen der Titelleisten-Schaltfläche angepasst wurden (s. S. 49).

ERWEITERUNGEN UND PLUG-INS

Kaspersky Password Manager besitzt Erweiterungskomponenten (Plug-ins), die in Programme integriert werden, für die eine Authentifizierung erforderlich ist. Sie können die Plug-ins für die von Ihnen benötigten Webbrowser selbst installieren. Installierte Plug-ins gewährleisten den Zugriff auf die Funktionen von Kaspersky Password Manager aus aus der Oberfläche eines Programms / Webbrowsers.

ZEIGER

Der Zeiger des Kaspersky Password Managers erlaubt es, ein Programm / eine Webseite schnell für das automatische Ausfüllen persönlicher Daten auszuwählen.

Gehen Sie folgendermaßen vor, um den Zeiger von Kaspersky Password Manager zu verwenden:

1. Führen Sie den Cursor auf das Symbol von Kaspersky Password Manager im Infobereich der Taskleiste und warten Sie einige Sekunden.
2. Ziehen Sie den erscheinenden Zeiger von Kaspersky Password Manager in das entsprechende Fenster des Programms / der Webseite. Kaspersky Password Manager ermittelt automatisch eine Aktion für das ausgewählte Programm / die Webseite.

KENNWORT-DATENBANK VERWALTEN

In der Kennwort-Datenbank sind alle Benutzerkonten für Programme und Web-Seiten mit einem oder mehreren Benutzernamen gespeichert. Außerdem enthält sie Visitenkarten (die z.B. Kontaktdaten, Telefonnummern, Nummern von Instant Messengern usw. enthalten).

Die Arbeit mit der Kennwort-Datenbank ist nur möglich, wenn sie nicht blockiert ist (s. S. 22). Bevor die Kennwort-Datenbank verändert wird, sollten die Einstellungen für das Backup der Datenbank (s. S. 42) angepasst werden. Wenn die Daten versehentlich verändert oder gelöscht wurden, verwenden Sie die Wiederherstellung der Kennwort-Datenbank (s. S. 34).

Sie können folgende Aktionen ausführen:

- persönliche Daten hinzufügen (s. S. 23), ändern (s. S.) und löschen (s. S. 32).
- Kennwort-Datenbank importieren / exportieren (s. S. 33) oder wiederherstellen (s. S. 34).

IN DIESEM ABSCHNITT

ZUGRIFF AUF DIE KENNWORT-DATENBANK

Für den Zugriff auf die Kennwort-Datenbank kann eine der folgenden Authentifizierungsmethode ausgewählt werden.

- **Schutz durch ein Master-Kennwort**. Für den Zugriff auf die Kennwort-Datenbank wird ein Master-Kennwort verwendet.
- **USB-Gerät**. Für den Zugriff auf die Kennwort-Datenbank wird ein Gerät mit USB-Anschluss verwendet, das an den Computer angeschlossen wird. Wenn das USB-Gerät getrennt wird, wird die Kennwort-Datenbank automatisch blockiert.
- **Bluetooth-Gerät**. Für den Zugriff auf die Kennwort-Datenbank wird ein Bluetooth-Gerät verwendet, das an Ihren Computer angeschlossen wird. Wenn das Bluetooth-Gerät getrennt wird, wird die Kennwort-Datenbank automatisch blockiert.
- **Ohne Authentifizierung**. Der Zugriff auf die Kennwort-Datenbank ist nicht geschützt.

In der Grundeinstellung ist der Schutz durch ein Master-Kennwort eingestellt, womit es ausreichend ist, sich nur ein Kennwort zu merken.

Das Master-Kennwort ist eine wichtige Methode für den Schutz Ihrer persönlichen Daten. Wenn als Authentifizierungsmethode ein Gerät ausgewählt wurde und dieses Gerät nicht verfügbar ist (oder z.B. verloren wurde), können Sie das Master-Kennwort verwenden, um auf Ihre persönlichen Daten zuzugreifen.

In der Grundeinstellung blockiert Kaspersky Password Manager die Kennwort-Datenbank beim Programmstart und nachdem der Computer für einen bestimmten Zeitraum inaktiv war (s. S. 44). Die Arbeit mit dem Programm ist nur möglich, wenn die Kennwort-Datenbank nicht blockiert ist.

Sie können die Kennwort-Datenbank auch auf folgende Arten freigeben / blockieren:

- im Fenster Kaspersky Password Manager (s. S. 19).
- mit einem USB- oder Bluetooth-Gerät – wird nur für die Authentifizierungsmethode mit einem USB- oder Bluetooth-Gerät verwendet.
- durch Doppelklick auf das Programmsymbol (s. S. 47) – Dafür muss zusätzlich die Aktion bei Doppelklick festgelegt werden.
- aus dem Kontextmenü von Kaspersky Password Manager (s. S. 18).
- mit der Tastenkombination STRG+ALT+L (s. S. 40).

Zur Eingabe des Master-Kennworts können Sie die virtuelle Tastatur verwenden, mit der Kennwörter ohne die herkömmliche Tastatur eingegeben werden können.

➡ *Gehen Sie folgendermaßen vor, um das Programm aus dem Kontextmenü des Programms zu blockieren:*

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Symbol von Kaspersky Password Manager.
2. Wählen Sie im folgenden Menü den Punkt **Blockieren**.

➡ *Gehen Sie folgendermaßen vor, um die Kennwort-Datenbank aus dem Kontextmenü freizugeben:*

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Symbol von Kaspersky Password Manager.
2. Wählen Sie im folgenden Menü den Punkt **Freigeben**.
3. Geben Sie im folgenden Fenster das Master-Kennwort ein.

PERSÖNLICHE DATEN HINZUFÜGEN

Persönliche Daten können nur hinzugefügt werden, wenn die Kennwort-Datenbank nicht blockiert ist (s. S. 22). Ein neues Benutzerkonto wird beim Start eines Programms / einer Webseite automatisch erkannt, wenn es nicht in der Kennwort-Datenbank gefunden wurde. Nach der Authentifizierung in einem Programm / auf einer Webseite schlägt Kaspersky Password Manager dann vor, die persönlichen Daten zur Kennwort-Datenbank hinzuzufügen.

In der Kennwort-Datenbank werden folgende Typen von persönlichen Daten unterschieden:

- **Benutzerkonto**. Kombination aus Benutzernamen und Kennwort für die Authentifizierung auf einer Webseite oder in einem Programm.
- **Gruppe von Benutzerkonten**. Sie dienen der bequemen Organisation von Benutzerkonten in der Kennwort-Datenbank.
- **Benutzername**. Kaspersky Password Manager schlägt in der Grundeinstellung vor, ein Benutzerkonto mit einem Benutzernamen zu erstellen. Ein zusätzlicher Benutzername wird verwendet, wenn Programme oder Webseiten es erlauben, mehrere Benutzernamen für den Zugriff auf ihre Ressourcen anzulegen.

- **Visitenkarte**. Sie dienen zum Speichern von Daten wie Geschlecht, Geburtsdatum, Kontaktinformationen, Telefonnummer, Arbeitsplatz, Nummer eines Instant Messengers, Homepage-Adresse usw. Um geschäftliche und private Informationen zu trennen, können Sie mehrere Visitenkarten anlegen.
- **Persönliche Notiz**. Dient zum Speichern beliebiger Informationen.

BENUTZERKONTO

Kaspersky Password Manager erkennt ein neues Benutzerkonto automatisch, wenn es nicht in der Kennwort-Datenbank gefunden wurde. Nach Abschluss der Authentifizierung in einem Programm / auf einer Webseite schlägt Kaspersky Password Manager vor, die Daten in der Kennwort-Datenbank zu speichern. Sie können ein neues Benutzerkonto auch manuell zur Kennwort-Datenbank hinfügen.

Ein Benutzerkonto enthält folgende Daten:

- Typ des Benutzerkontos (Benutzerkonto für ein Programm oder Benutzerkonto für das Internet)
- Benutzername / mehrere Benutzernamen
- Kennwort
- Pfad des Programms / Webadresse der Webseite im Internet (abhängig vom Typ des Benutzerkontos)
- Einstellungen für die Verknüpfung des Benutzerkontos mit einem Objekt
- Einstellungen für die Aktivierung des Benutzerkontos
- Kommentar
- Einstellungen für das Ausfüllen zusätzlicher Felder auf einer Webseite

Kaspersky Password Manager erlaubt es, ein oder mehrere Benutzerkonten für die Authentifizierung in einem Programm oder auf einer Webseite zu verwenden.

Auf Basis des Pfads für ein Programm oder der Webadresse für eine Webseite kann mit Hilfe von Kaspersky Password Manager ein Bereich für die Verwendung eines Benutzerkontos festgelegt werden.

Es bestehen folgende Möglichkeiten, um ein Benutzerkonto hinzuzufügen:

- Titelleisten-Schaltfläche – Dazu wird im Menü der Titelleisten-Schaltfläche der Punkt **Benutzerkonto hinzufügen** ausgewählt.
- aus dem Kontextmenü von Kaspersky Password Manager – Dazu dient der Punkt **Benutzerkonto hinzufügen** im Kontextmenü von Kaspersky Password Manager.
- aus dem Hauptfenster von Kaspersky Password Manager.

➡ *Gehen Sie folgendermaßen vor, um vom Hauptfenster aus ein neues Benutzerkonto hinzuzufügen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Klicken Sie im folgenden Fenster oben auf **Hinzufügen** und wählen Sie den Punkt **Benutzerkonto hinzufügen**.
4. Wählen Sie im folgenden Assistentenfenster einen Typ für das Benutzerkonto aus (Benutzerkonto für das Internet, Benutzerkonto für ein Programm oder benutzerdefinierter Modus) und klicken Sie auf **Weiter**.
   - Wenn Sie ein Benutzerkonto für das Internet oder für ein Programm ausgewählt haben, geben Sie eine Webseite oder ein Programm an, für das dieses Benutzerkonto dienen soll, und klicken Sie auf **Weiter**.

- Wenn Sie den erweiterten Modus ausgewählt haben, geben Sie auf der Registerkarte **Links** einen Programmpfad / eine Webseite an und passen Sie die Verwendung des Benutzerkontos an.

5. Geben Sie im oberen Fensterbereich im Feld **Name** einen Namen für das neue Benutzerkonto ein oder ändern Sie den Namen.

6. Geben Sie auf der Registerkarte **Zugangsdaten** den Benutzernamen und das Kennwort an.

   Ein Benutzername kann aus einem oder mehreren Wörtern bestehen. Um für einen Benutzernamen Schlüsselwörter festzulegen (s. S. 25) klicken Sie auf die Schaltfläche .

   Um einen Benutzernamen / ein Kennwort in die Zwischenablage zu kopieren, klicken Sie auf .

   Um einen Benutzernamen aus einem anderen Benutzerkonto zu kopieren, verwenden Sie den Link **Benutzername eines anderen Benutzerkontos verwenden**.

   Um automatisch ein neues Kennwort zu erstellen, klicken Sie auf den Link **Neues Kennwort generieren** (s. S. 50).

7. Passen Sie bei Bedarf auf der Registerkarte **Formular manuell ändern** die Einstellungenfür das Ausfüllen von anderen Feldern auf einer Webseite an.

8. Geben Sie bei Bedarf auf der Registerkarte **Kommentar** eine Erläuterung für das Benutzerkonto an. Damit der Damit ein Kommentar nach der Aktivierung des Benutzerkontos in einer Meldung erscheint, aktivieren Sie das Kontrollkästchen **Kommentare in Meldung anzeigen**.

SCHLÜSSELWÖRTER FÜR DIE SUCHE FESTLEGEN

Zur schnellen Suche nach persönlichen Daten in der Kennwort-Datenbank können Schlüsselwörter verwendet werden. Sie werden für jeden Benutzernamen angelegt. Es wird empfohlen, die Schlüsselwörter beim Hinzufügen eines Benutzerkontos (s. S. 24) / Benutzernamens (s. S. 29) festzulegen.

Gehen Sie folgendermaßen vor, um Schlüsselwörter für einen Benutzernamen festzulegen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.

3. Wählen Sie einen Benutzernamen aus der Liste **Meine Kennwörter** aus und klicken Sie im oberen Fensterbereich auf **Ändern**.

4. Klicken Sie im folgenden Fenster auf die Schaltfläche neben dem Feld **Benutzername** und geben Sie im Feld **Beschreibung** die Schlüsselwörter ein.

   Wenn ein Benutzerkonto mit einem Benutzernamen ausgewählt wurde, klicken Sie im folgenden Fenster **Benutzerkonto mit einem Benutzernamen** auf der Registerkarte **Zugangsdaten** auf die Schaltfläche .

PFAD EINES PROGRAMMS/ EINER WEBSEITE HINZUFÜGEN

Um ein Benutzerkonto mit einem Programm oder einer Webseite zu assoziieren, muss ein Link erstellt werden. Für eine Webseite besteht der Link aus einer Webadresse, für ein Programm aus dem Pfad einer ausführbaren Programmdatei auf dem Computer. Ohne diese Angaben wird ein Benutzerkonto nicht mit einem Programm / einer Webseite verknüpft.

Es gibt folgende Methoden, um ein Programm / eine Webseite mit einem Benutzerkonto zu verknüpfen:

- Mit der Schaltfläche wird ein Link aus der Liste der ausgewählten Webseiten Ihres Webbrowsers oder aus der Liste der Programme auf Ihrem Computer ausgewählt.
- manuelle Angabe des Pfads eines Programms / einer Webseite
- Verwendung des Zeigers von Kaspersky Password Manager.

Um die Korrektheit eines eingegebenen Pfads zu prüfen, starten Sie das Programm / die Webseite mit der Schaltfläche .

Gehen Sie folgendermaßen vor, um einen Link aus der Liste auszuwählen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Klicken Sie im oberen Fensterbereich auf **Hinzufügen** und wählen Sie den Punkt **Benutzerkonto hinzufügen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Links** im Feld **Link** auf die Schaltfläche .
5. Geben Sie im folgenden Fenster im Feld **Link** den Pfad für das Programm / für die Webseite an.

   Um eine Webseite aus der Liste der gespeicherten Webseiten (Lesezeichen) anzugeben, wählen Sie die Webseite in der Liste **Lesezeichen** aus und klicken Sie auf den Link **Link aus Favoriten kopieren**. Um den Pfad einer Webseite aus dem Browserfenster zu kopieren, klicken Sie auf den Link **Pfad des verknüpften Programms verwenden**.

   Um einen Link zu einem Programm zu erstellen, klicken Sie im Feld **Link** auf und geben Sie den Pfad der ausführbaren Programmdatei an.

Gehen Sie folgendermaßen vor, um den Pfad eines Programms / einer Webseite manuell anzugeben:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Klicken Sie im oberen Fensterbereich auf **Hinzufügen** und wählen Sie den Punkt **Benutzerkonto hinzufügen**.
4. Geben Sie im folgenden Fenster auf der Registerkarte **Links** im Feld **Link** den Pfad des Programms / die Adresse der Webseite an. Die Adresse einer Webseite muss mit http://www beginnen.

Gehen Sie folgendermaßen vor, um den Pfad eines Programms / einer Webseite mit dem Zeiger von Kaspersky Password Manager anzugeben:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Klicken Sie im oberen Fensterbereich auf **Hinzufügen** und wählen Sie den Punkt **Benutzerkonto hinzufügen**.

4. Geben Sie im folgenden Fenster auf der Registerkarte **Links** im Feld **Link** den Pfad des Programms / der Webseite an. Führen Sie dazu den Zeiger von Kaspersky Password Manager in das Fenster des Programms / des Webbrowsers.

METHODE FÜR DIE VERKNÜPFUNG EINES BENUTZERKONTOS AUSWÄHLEN

Um zu ermitteln, aus welchem Benutzerkonto beim Start eines Programms / einer Webseite automatisch Daten eingetragen werden sollen, verwendet Kaspersky Password Manager den Pfad eines Programms / die Webadresse einer Webseite.

Da Kaspersky Password Manager es erlaubt, mehrere Benutzerkonten für ein Programm / eine Webseite zu verwenden, ist es erforderlich, für jedes Benutzerkonto einen Verwendungsbereich festzulegen.

Auf Basis des Pfads für ein Programm / der Webadresse für eine Webseite kann mit Hilfe von Kaspersky Password Manager ein Bereich für die Verwendung eines Benutzerkontos festgelegt werden. Die Einstellungen für den Bereich werden beim Erstellen eines Benutzerkontos (s. S. 24) angepasst. Diese Werte können später geändert werden.

Die Varianten für die Verwendung eines Benutzerkontos unterscheiden sich in Abhängigkeit des Objekts (Programm oder Webseite).

Für ein Programm bestehen folgende Varianten:

- Benutzerkonto für ein Programm verwenden. Das Benutzerkonto wird für alle Programmfenster verwendet, die Eingabefelder für persönliche Daten besitzen.
- Nach Fenstertitel erkennen. Das Benutzerkonto wird nur für das angegebene Fenster des Programms verwendet.

  Ein Programm kann beispielsweise mehrere Benutzerkonten verwenden. Für die einzelnen Benutzerkonten unterscheiden sich in einem Programm nur die Fenstertitel. Kaspersky Password Manager trägt auf Basis des Titels eines Programmfensters automatisch die Daten eines Benutzerkontos ein.

Für Webseiten bestehen folgende Varianten für die Verwendung eines Benutzerkontos:

- Nur für die angegebene Webseite. Benutzername und Kennwort werden von Kaspersky Password Manager nur auf der Webseite mit der angegebenen Adresse automatisch in die Authentifizierungsfelder eingefügt.

  Wenn ein Benutzerkonto beispielsweise mit einer Webseite der Adresse http://www.web-site.com/login.html verknüpft ist, gilt dieses Benutzerkonto nicht für andere Webseiten dieser Webseite (z.B. für http://www.web-site.com/index.php).
- Für Webseiten aus einem Ordner. Kaspersky Password Manager fügt Benutzername und Kennwort automatisch in die Authentifizierungsfelder für alle Webseiten des letzten Ordners ein.

  Wenn beispielsweise die Adresse der Webseite http://www.web-site.com/cgi-bin/login.html eingegeben wurde, wird dieses Benutzerkonto für alle Webseiten im Ordner *cgi-bin* verwendet.
- Für eine Webseite: <Domänenname ab Third Level oder niedriger>. Dieses Benutzerkonto wird für eine beliebige Webseite der Domäne verwendet (:<ab Third-Level-Domain oder niedriger>).

  Kaspersky Password Manager fügt beispielsweise automatisch die Zugangsdaten für folgende Webseiten ein: http://www.domain1.domain2.web-site.com/login.html oder http://www.domain1.domain2.web-site.com/index.php. Dieses Benutzerkonto wird allerdings nicht verwendet für Webseiten mit Adressen, die verschiedene Fourth-Level-Domains besitzen: http://www.domain3.domain2.web-site.com/index.php oder http://www.domain4.domain2.web-site.com/index.php.
- Für eine Webseite: <Name der Webseite>. Dieses Benutzerkonto wird für alle Seiten einer Webseite verwendet, die Eingabefelder für Benutzername und Kennwort besitzen.

  Kaspersky Password Manager fügt beispielsweise automatisch die Zugangsdaten für folgende Webseiten ein: http://www.domain1.domain2.web-site.com/login.html, http://www.domain2.domain2.web-site.com/index.php, http://www.domain3.domain2.web-site.com/index.php oder http://www.domain4.domain2.web-site.com/index.php.

Gehen Sie folgendermaßen vor, um die Parameter für die Verwendung eines Benutzerkontos festzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Wählen Sie ein Benutzerkonto aus der Liste **Meine Kennwörter** aus und klicken Sie auf **Ändern**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Links** eine Variante für die Verwendung des Benutzerkontos.

BENUTZERKONTO AUTOMATISCH AKTIVIEREN

Die automatische Aktivierung eines Benutzerkontos ist standardmäßig aktiviert. Kaspersky Password Manager fügt nur Benutzername und Kennwort in die Authentifizierungsfelder ein. Sie können die Aktivierungsparameter eines Benutzerkontos anpassen (s. S. 24).

Für Webseiten wird zusätzlich der Bereich der Webadressen angegeben, für den die automatische Aktivierung verwendet werden soll.

Es bestehen folgende Varianten für die Aktivierung eines Benutzerkontos:

- Nur für eine angegebene Webseite. Das Benutzerkonto wird nur für diese Webseite aktiviert.
- Für eine Webseite. Das Benutzerkonto wird für alle Webseiten einer Webseite aktiviert.

Gehen Sie folgendermaßen vor, um die automatische Aktivierung eines Benutzerkontos festzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Wählen Sie ein Benutzerkonto aus der Liste **Meine Kennwörter** aus und klicken Sie auf **Ändern**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Links** das Kontrollkästchen **Benutzerkonto nach dem Laden automatisch aktivieren**.

   Wählen Sie für eine Webseite zusätzlich eine Aktivierungsmethode für das Benutzerkonto.

ZUSATZFELDER AUSFÜLLEN

Bei der Authentifizierung auf einer Webseite werden neben Kennwort und Benutzername manchmal auch andere Daten abgefragt. Kaspersky Password Manager erlaubt es, Zusatzfelder automatisch auszufüllen. Sie können die Einstellungen für das automatische Ausfüllen von Zusatzfeldern für ein Benutzerkonto anpassen.

Die Einstellungen für Zusatzfelder können dann angepasst werden, wenn für ein Benutzerkonto der Pfad eines Programms / die Adresse einer Webseite angegeben ist.

Um die Einstellungen der Felder anzupassen, lädt Kaspersky Password Manager die Webseite vorübergehend und analysiert dann alle Felder und Schaltflächen. Felder und Schaltflächen werden für jede Webseite in Gruppen eingeteilt.

Während der Arbeit mit einer geladenen Webseite speichert Kaspersky Password Manager vorübergehend Dateien und Bilder auf Ihrem Computer.

Gehen Sie folgendermaßen vor, um die Parameter für Zusatzfelder anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Wählen Sie ein Benutzerkonto aus der Liste **Meine Kennwörter** aus und klicken Sie auf **Ändern**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Formular manuell ändern** auf den Link **Klicken Sie, um die Werte der Felder zu ändern.**
5. Aktivieren Sie im folgenden Fenster **Formular manuell ändern** oben das Kontrollkästchen für das entsprechende Feld / Schaltfläche.
6. Aktivieren Sie durch Doppelklick das Feld in der Spalte **Wert** für ein ausgewähltes Feld / eine Schaltfläche.

GRUPPE FÜR BENUTZERKONTEN ERSTELLEN

Die Verwendung von Gruppen für Benutzerkonten ist hilfreich bei der Organisation von Informationen in der Kennwort-Datenbank. Eine Gruppe besteht aus einem Ordner, der hinzugefügte Benutzerkonten enthält.

Erstellte Gruppen werden im Kontextmenü von Kaspersky Password Manager angezeigt:
Punkt **Benutzerkonten** → **<Name der Gruppe>**.

Gehen Sie folgendermaßen vor, um eine Gruppe für Benutzerkonten zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Klicken Sie im oberen Fensterbereich auf **Hinzufügen** und wählen Sie den Punkt **Gruppe hinzufügen**.
4. Geben Sie einen Namen für die neue Gruppe ein.
5. Fügen Sie dem neuen Ordner Benutzerkonten aus der Liste **Meine Kennwörter** hinzu. Die Konten werden mit der Maus in den Ordner gezogen.

BENUTZERNAME

Für die Arbeit mit einigen Programmen / Webseiten werden häufig mehrere Benutzernamen verwendet. Kaspersky Password Manager erlaubt es, mehrere Benutzernamen für ein Benutzerkonto zu speichern. Kaspersky Password Manager erkennt einen neuen Benutzernamen automatisch bei der ersten Verwendung und schlägt vor, ihn zu dem Benutzerkonto für dieses Programm / diese Webseite hinzuzufügen. Sie können einen neuen Benutzernamen manuell für ein Benutzerkonto hinzufügen und ihn später ändern. Außerdem können Sie einen Benutzernamen für unterschiedliche Benutzerkonten verwenden.

Es bestehen folgende Möglichkeiten, um einen neuen Benutzernamen für ein Benutzerkonto hinzuzufügen:

- mit der Titelleisten-Schaltfläche. Wählen Sie dazu im Menü der Titelleisten-Schaltfläche den Punkt **Benutzerkonten** –> **Benutzerkonto ändern** –> **Benutzername hinzufügen**.
- aus dem Programmhauptfenster.

Gehen Sie folgendermaßen vor, um einen Benutzernamen für ein Benutzerkonto hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.

3. Wählen Sie ein Benutzerkonto aus der Liste **Meine Kennwörter** aus, klicken Sie auf **Hinzufügen** und wählen Sie den Punkt **Benutzername hinzufügen**.

4. Geben Sie im folgenden Fenster einen Benutzernamen und ein Kennwort ein. Ein Benutzername kann aus einem oder mehreren Wörtern bestehen. Um für einen Benutzernamen Schlüsselwörter festzulegen, klicken Sie auf die Schaltfläche und füllen Sie dann das Feld **Beschreibung** aus.

   Um einen Benutzernamen / ein Kennwort in die Zwischenablage zu kopieren, verwenden Sie die Schaltfläche . Um automatisch ein Kennwort zu erstellen, verwenden Sie den Link **Neues Kennwort generieren** (s. S. 50).

   Um einen Benutzernamen aus einem anderen Benutzerkonto zu kopieren, verwenden Sie den Link **Benutzername eines anderen Benutzerkontos verwenden**.

VISITENKARTE

Für die Anmeldung auf einer Webseite werden neben Benutzername und Kennwort häufig noch andere persönliche Daten verwendet (z.B. Vor- und Nachname, Geburtsjahr, Geschlecht, E-Mail-Adresse, Telefonnummer, Land u.a.). Kaspersky Password Manager erlaubt es, die gesamten Daten in Form von Visitenkarten in der verschlüsselten Kennwort-Datenbank zu speichern. Bei der Anmeldung auf einer neuen Webseite füllt Kaspersky Password Manager auf Grundlage der Daten aus einer ausgewählten Visitenkarte automatisch das Anmeldeformular aus. Um beim Speichern geschäftliche und private Informationen zu trennen, können mehrere Visitenkarten angelegt werden. Die Einstellungen einer Visitenkarte können später geändert werden.

➡ *Gehen Sie folgendermaßen vor, um eine Visitenkarte anzulegen:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie auf **Password Manager**.

3. Klicken Sie im oberen Fensterbereich auf **Hinzufügen** –> **Visitenkarte hinzufügen**.

4. Geben Sie im folgenden Fenster im Feld **Name** einen Namen für die Visitenkarte an.

5. Geben Sie für die entsprechenden Felder einen Wert ein. Ein Feld wird durch Doppelklick auf die Spalte **Wert** aktiviert.

PERSÖNLICHE NOTIZ

Persönliche Notizen dienen dazu, Textinformationen in verschlüsselter Form zu speichern (z.B. Passdaten, Kontonummern usw.) und schnell auf die gespeicherten Daten zuzugreifen. Kaspersky Password Manager bietet eine Auswahl von Standardwerkzeugen zur Bearbeitung von persönlichen Notizen. Beim Erstellen einer persönlichen Notiz können Vorlagen mit einer Auswahl von standardmäßigen Datentypen (s. S. 46) verwendet werden.

Die Einstellungen für eine persönliche Notiz können später geändert werden.

➡ *Gehen Sie folgendermaßen vor, um eine persönliche Notiz ohne Vorlage zu erstellen:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie auf **Password Manager**.

3. Klicken Sie im oberen Fensterbereich auf **Hinzufügen** –> **Persönliche Notiz hinzufügen**.

4. Geben Sie im folgenden Fenster im Feld **Name** einen Namen für die persönliche Notiz ein.

5. Geben Sie die entsprechenden Informationen im Texteditor ein.

➧ *Gehen Sie folgendermaßen vor, um eine persönliche Notiz auf Basis einer Vorlage zu erstellen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Klicken Sie im oberen Fensterbereich auf **Hinzufügen** –> **Persönliche Notiz hinzufügen**.
4. Geben Sie im folgenden Fenster im Feld **Name** einen Namen für die persönliche Notiz ein.
5. Klicken Sie im unteren Fensterbereich auf **Vorlage auswählen** und wählen Sie die entsprechende Vorlage aus.
6. Tragen Sie die erforderlichen Daten ein und formatieren Sie den Text entsprechend.

➧ *Um eine persönliche Notiz anzuzeigen,*

öffnen Sie das Kontextmenü des Kaspersky Password Managers und wählen Sie den Punkt **Persönliche Notizen** → **<Name der Gruppe>** → **<Name der persönlichen Notiz>**.

PERSÖNLICHE DATEN VERWENDEN

Kaspersky Password Manager verknüpft Benutzerkonten mit Programmen / Webseiten, für die sie verwendet werden. Beim Start eines Programms / einer Webseite erfolgt in der Kennwort-Datenbank automatisch eine Suche nach einem verknüpften Benutzerkonto. Wenn ein Benutzerkonto gefunden wird, werden die persönlichen Daten automatisch eingetragen. Wenn die Kennwort-Datenbank kein verknüpftes Benutzerkonto enthält, schlägt Kaspersky Password Manager vor, es zur Kennwort-Datenbank hinzuzufügen (s. S. 24).

Einige Programme / Webseiten können mehrere Benutzernamen verwenden. Kaspersky Password Manager erlaubt es, mehrere Benutzernamen für ein Benutzerkonto zu speichern.

Wenn bei der Authentifizierung ein neuer Benutzername verwendet wurde, schlägt der, Kaspersky Password Manager vor, ihn für das gestartete Programm / für die gestartete Webseite dem Benutzerkonto hinzuzufügen (s. S. 29). In diesem Fall erscheint beim Start eines Programms / einer Webseite neben den Eingabefeldern für persönliche Daten ein Fenster mit einer Liste der Benutzernamen für dieses Benutzerkonto.

Neben Benutzername und Kennwort werden für die Anmeldung auf einer Webseite häufig noch andere persönliche Daten verwendet (z.B. Vor- und Nachname, Geschlecht, Land, Stadt, Telefon, E-Mail-Adresse u.a.). Kaspersky Password Manager speichert solche Daten in Form von Visitenkarten in der verschlüsselten Kennwort-Datenbank.

Um geschäftliche und private Informationen zu trennen, können Sie mehrere Visitenkarten anlegen (s. S. 30). Bei der Anmeldung in einem Programm / auf einer Webseite füllt Kaspersky Password Manager dann auf Grundlage der Daten aus einer ausgewählten Visitenkarte automatisch die Felder des Anmeldeformulars aus. Es ergibt sich eine Zeitersparnis, weil sich wiederholende Anmeldeformulare nicht manuell ausgefüllt werden müssen.

Bei der Authentifizierung in einem Programm / auf einer Webseite füllt Kaspersky Password Manager die persönlichen Daten nur dann aus, wenn die Kennwort-Datenbank nicht blockiert ist.

Ein Benutzerkonto kann auf folgende Arten verwendet werden:

- Programm / Webseite starten. Das Authentifizierungsformular wird auf Grundlage der Daten des Benutzerkontos automatisch ausgefüllt.
- Zeiger von Kaspersky Password Manager verwenden. Führen Sie dazu den Cursor auf das Programmsymbol im Infobereich der Taskleiste und aktivieren Sie das Benutzerkonto anschließend, indem Sie den Zeiger von Kaspersky Password Manager in das Fenster des entsprechenden Programms / der Webseite ziehen.
- Benutzerkonto in der Liste der häufig verwendeten Benutzerkonten auswählen. Öffnen Sie dazu das Kontextmenü von Kaspersky Password Manager und wählen Sie im Block der häufig verwendeten Benutzerkonten einen Eintrag aus.

- Kontextmenü von Kaspersky Password Manager verwenden. Öffnen Sie dazu das Kontextmenü von Kaspersky Password Manager und wählen Sie den Punkt **Benutzerkonten** → **<Name des Benutzerkontos>** aus.

➡ *Gehen Sie folgendermaßen vor, um eine Visitenkarte zu verwenden:*

1. Klicken Sie im Fenster des Programms / Webbrowsers rechts oben auf die Titelleisten-Schaltfläche.
2. Wählen Sie im folgenden Menü den Punkt **Visitenkarten** – > **<Name der Visitenkarte>** aus. Kaspersky Password Manager füllt auf Grundlage der Daten aus der Visitenkarte automatisch die Anmeldefelder der Webseite aus.

KENNWÖRTER SUCHEN

Die Suche nach persönlichen Daten kann in folgenden Fällen erschwert werden:

- Bestimmte Kennwörter sind nicht mit Programmen / Webseiten verknüpft.
- Die Kennwort-Datenbank enthält eine große Anzahl von Benutzerkonten.

Mit Hilfe von Kaspersky Password Manager lassen sich Kennwörter schnell nach folgenden Parametern auffinden:

- Name des Benutzerkontos
- Benutzername
- Schlüsselwörter (s. S. 25) (Kriterien für Suche nach Schlüsselwörtern werden zusätzlich für jeden Benutzernamen eingestellt).
- Webadresse (für Webseiten)

Es kann nach einem gesamten Namen, nach Anfangsbuchstaben oder beliebigen Zeichen, die in dem Namen eines Benutzerkontos oder Links enthalten sind, gesucht werden.

➡ *Gehen Sie folgendermaßen vor, um ein Benutzerkonto zu suchen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Geben Sie im oberen Fensterbereich in der Suchzeile einen Text ein.

PERSÖNLICHE DATEN LÖSCHEN

Bevor irgendwelche Änderungen von persönlichen Daten erfolgen, legt Kaspersky Password Manager automatisch eine Sicherungskopie der Kennwort-Datenbank an. Wenn die Daten versehentlich verändert oder gelöscht wurden, verwenden Sie die Wiederherstellung der Kennwort-Datenbank (s. S. 34).

Es können ein oder alle Elemente aus der Kennwort-Datenbank gelöscht werden.

➡ *Gehen Sie folgendermaßen vor, um ein Element aus der Kennwort-Datenbank zu löschen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Wählen Sie ein Element aus der Liste **Meine Kennwörter** aus, klicken Sie auf **Löschen** und wählen Sie den Punkt **Löschen**.

Gehen Sie folgendermaßen vor, um alle Elemente aus der Kennwort-Datenbank zu löschen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Wählen Sie ein Element aus der Liste **Meine Kennwörter** aus, klicken Sie auf **Löschen** und wählen Sie den Punkt **Alle löschen**.

DATEN IMPORTIEREN/EXPORTIEREN

Kaspersky Password Manager erlaubt den Import und Export Ihrer Kennwort-Datenbank sowie einzelner Objekte der Kennwort-Datenbank (Visitenkarten, Benutzerkonten oder persönliche Notizen).

Geladen werden können sowohl Kennwörter aus anderen Programmen zur Kennwort-Verwaltung (z.B. aus Internet Explorer, Mozilla Firefox, KeePass) als auch Kennwörter, die Sie früher mit Kaspersky Password Manager gespeichert haben.

Der Import von Kennwörtern erfolgt aus Dateien der Formate xml und ini.

Kaspersky Password Manager erlaubt es, eine Kennwort-Datenbank in einer Datei des Formats xml, html oder txt zu speichern.

Das Speichern eines Kennworts in einer Datei ist vorteilhaft, um den gemeinsamen Zugriff auf Kennwörter zu gewährleisten, um die Kennwort-Datenbank auszudrucken oder um eine Sicherungskopie der Kennwort-Datenbank in einem anderen Dateiformat (als dem Format von Kaspersky Password Manager) zu speichern.

Gespeicherte Kennwörter werden in unverschlüsselten Dateien gespeichert und sind nicht vor unerlaubtem Zugriff geschützt. Es wird deshalb empfohlen, rechtzeitig zu überlegen, wie die exportierten Daten geschützt werden können.

Die Kennwort-Datenbank wird beim Import verändert. Sie können auswählen, welche der folgenden Aktionen mit der Kennwort-Datenbank ausgeführt werden soll:

- **Überschreiben**. Die aktuelle Kennwort-Datenbank wird durch die geladene ersetzt (alle Kennwörter, die vor dem Laden in der Kennwort-Datenbank des Kaspersky Password Managers gespeichert waren, werden gelöscht).
- **Verbinden**. Die geladenen Kennwörter werden zur Kennwort-Datenbank hinzugefügt. Beim Zusammenführen können Sie auswählen, welche Benutzerkonten in den Kaspersky Password Manager geladen werden sollen.
- **Abbrechen**. Der Laden der Kennwörter wird abgebrochen.

Gehen Sie folgendermaßen vor, um Kennwörter aus einer Datei zu laden:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Klicken Sie im unteren Bereich auf den Link **Kennwörter laden**.
4. Wählen Sie im folgenden Fenster **Kennwörter laden** das Programm, aus dem Kennwörter importiert werden sollen, und klicken Sie auf **Kennwörter laden**.
5. Geben Sie im folgenden Fenster die Datei mit Kennwörtern an, die Sie laden möchten, und klicken Sie auf **Öffnen**.
6. Wählen Sie im folgenden Fenster eine Aktion für die Kennwort-Datenbank aus.

Gehen Sie folgendermaßen vor, um die Kennwort-Datenbank in einer Datei zu speichern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Klicken Sie im unteren Bereich auf den Link **Speichern**.
4. Wählen Sie im folgenden Fenster eine Speicherungsmethode aus (Speicherung der gesamten Kennwort-Datenbank oder von ausgewählten Objekten) und klicken Sie auf **Weiter**.
5. Wählen Sie im folgenden Fenster die Speicherungseinstellungen aus.
   - Wenn Sie die zu speichernden Daten schützen möchten, wählen Sie die Variante **Sicheres Speichern** aus und legen Sie ein Kennwort für den Datenschutz fest.
   - Wenn Sie die Daten in einer unverschlüsselten Datei speichern möchten, wählen Sie die Variante **Unverschlüsseltes Speichern** aus und geben Sie ein Dateiformat für die Speicherung an.
   - Um eine Änderung des Kennworts für die gespeicherten Daten zu planen, aktivieren Sie das Kontrollkästchen **Änderung des Kennworts für gespeicherte Objekte planen** und wählen Sie ein Datum aus, zu dem das Kennwort zurückgesetzt wird und Kaspersky Password Manager Sie darüber benachrichtigen soll, dass das Kennwort geändert werden muss.
6. Geben Sie im folgenden Fenster einen Pfad an, unter dem die Datei gespeichert werden soll, und klicken Sie auf **Weiter**.
7. Prüfen Sie im folgenden Fenster die Einstellungen für die Datenspeicherung und starten Sie den Speichervorgang.

BACKUP / WIEDERHERSTELLUNG DER KENNWORT-DATENBANK

Bevor irgendwelche Änderungen in der Kennwort-Datenbank erfolgen, wird automatisch eine Sicherungskopie angelegt. Der Pfad, unter dem die Sicherungskopien gespeichert werden, ist standardmäßig vorgegeben. Sie können ihn jedoch ändern (s. S. 42). Eine Wiederherstellung von Kennwörtern kann in folgenden Fällen von Nutzen sein:

- wenn vorherige Änderungen rückgängig gemacht werden sollen.
- wenn die Kennwort-Datenbank überschrieben oder gelöscht wurde.
- wenn die aktuelle Kennwort-Datenbank aufgrund eines Hardware- oder Systemfehlers nicht verfügbar / beschädigt ist.

Alle Daten einer Sicherungskopie werden in verschlüsselter Form gespeichert. Kaspersky Password Manager protokolliert alle Veränderungen in der Kennwort-Datenbank. Im Programm werden die Sicherungskopien nach Datum sortiert in einer Liste angezeigt, wobei die letzte Kopie an erster Stelle steht. Für jede Sicherungskopie werden folgende Daten genannt:

- Speicherort
- Datum und Uhrzeit der Erstellung
- Veränderungen im Vergleich zur vorhergehenden Version

Sicherungskopien können für folgende Aufgaben verwendet werden:

- Wiederherstellung der Kennwort-Datenbank aus einer ausgewählten Sicherungskopie
- Löschen alter Versionen von Sicherungskopien
- Ändern des Speicherorts für Sicherungskopien (s. S. 42).

➡ *Gehen Sie folgendermaßen vor, um die Kennwort-Datenbank wiederherzustellen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Klicken Sie im unteren Bereich des Fensters auf den Link **Kennwort-Datenbank wiederherstellen**.
4. Wählen Sie im folgenden Fenster **Wiederherstellung** das Datum einer Sicherungskopie aus der Liste aus und klicken Sie im oberen Fensterbereich auf **Wiederherstellen**.
5. Bestätigen Sie die Wiederherstellung im folgenden Fenster durch Klick auf **OK**.

➡ *Gehen Sie folgendermaßen vor, um nicht mehr benötigte Versionen von Sicherungskopien zu löschen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Klicken Sie im unteren Bereich des Fensters auf den Link **Kennwort-Datenbank wiederherstellen**.
4. Wählen Sie im folgenden Fenster **Wiederherstellung** aus der Liste der Sicherungskopien jene Versionen, die gelöscht werden sollen. Halten Sie die Taste **STRG** gedrückt, um mehrere Versionen auszuwählen.
5. Klicken Sie auf **Löschen**.
6. Bestätigen Sie das Löschen der Sicherungskopien im folgenden Fenster durch Klick auf **OK**.

PROGRAMMEINSTELLUNGEN ANPASSEN

Die Programmeinstellungen können nur angepasst werden, wenn die Kennwort-Datenbank nicht blockiert ist (s. S. 22). Durch das Ändern der Einstellungen können Sie folgende Aktionen ausführen:

- Zeitpunkt für den Programmstart festlegen (s. S. 47).
- Meldungen aktivieren (s. S. 48).
- Benutzernamen festlegen (s. S. 37), der standardmäßig beim Erstellen eines neuen Benutzerkontos verwendet werden soll.
- Speicherdauer des Kennworts in der Zwischenablage festlegen (s. S. 48).
- Liste der häufig verwendeten Benutzerkonten anpassen (s. S. 38).
- Liste mit ignorierten Webseiten anlegen (s. S. 38), für die die Funktionen von Kaspersky Password Manager nicht verwendet werden.
- Liste mit vertrauenswürdigen Webseiten anlegen (s. S. 38), für die Kaspersky Password Manager eine Weiterleitung zulässt.
- Tastenkombinationen für den Schnellzugriff auf die Funktionen von Kaspersky Password Manager anpassen (s. S. 40).
- Speicherpfad für Kennwort-Datenbank (s. S. 40) und Sicherungskopien (s. S. 42) ändern.
- Methode zur Datenverschlüsselung ändern (s. S. 42).
- automatisches Blockieren der Kennwort-Datenbank anpassen (s. S. 44).
- Master-Kennwort ändern (s. S. 45).
- Zugriff auf die Kennwort-Datenbank anpassen (s. S. 44).
- Position der Titelleisten-Schaltfläche ändern, Liste der Programme anlegen, die die Titelleisten-Schaltfläche unterstützen (s. S. 49).
- Liste der unterstützten Programme anlegen (s. S. 46).

➡ *Gehen Sie folgendermaßen vor, um die Funktionsparameter von Kaspersky Password Manager zu ändern:*

1. Öffnen Sie das Programmhauptfenster. Klicken Sie im folgenden Fenster **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt aus, der geändert werden soll.
3. Nehmen Sie im rechten Fensterbereich für den ausgewählten Abschnitt die entsprechenden Änderungen vor.

IN DIESEM ABSCHNITT

STANDARDMÄßIGEN BENUTZERNAMEN VERWENDEN

Kaspersky Password Manager erlaubt es, einen Benutzernamen festzulegen, der beim Erstellen eines neuen Benutzerkontos automatisch im Feld **Benutzername** angezeigt wird (s. S. 24).

➡ *Gehen Sie folgendermaßen vor, um einen standardmäßigen Benutzernamen festzulegen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Bereich des folgenden Fensters den Abschnitt **Allgemein**.
4. Füllen Sie auf der rechten Fensterseite das Feld **Standardmäßiger Benutzername** aus.

HÄUFIG VERWENDETE BENUTZERKONTEN

Kaspersky Password Manager ermöglicht einen schnellen Zugriff auf Benutzerkonten. Eine Liste der häufig verwendeten Benutzerkonten wird im Programmhauptfenster angezeigt und kann außerdem im Kontextmenü und im Menü der Titelleisten-Schaltfläche angezeigt werden.

Die Liste enthält die Namen der Programme / Webseiten, die Sie am häufigsten starten. Die Elemente dieser Liste sind alphabetisch oder nach Verwendungshäufigkeit angeordnet.

Die Liste der häufig verwendeten Benutzerkonten ist im Menü verfügbar, wenn die Kennwort-Datenbank nicht blockiert ist (s. S. 22).

Sie können folgende Einstellungen für die Liste festlegen:

- **Anzahl der Elemente in der Liste** – Maximale Anzahl der häufig verwendeten Benutzerkonten, die im Kontextmenü des Programms angezeigt werden sollen.
- **Liste im Programm-Menü anzeigen** – Die Liste der häufig verwendeten Benutzerkonten ist im Kontextmenü von Kaspersky Password Manager verfügbar.
- **Liste im Menü der Titelleisten-Schaltfläche anzeigen** – Die Liste der häufig verwendeten Benutzerkonten ist im Menü der Titelleisten-Schaltfläche verfügbar (aus einem Programmfenster / Webbrowser).

➡ *Gehen Sie folgendermaßen vor, damit häufig verwendete Benutzerkonten im Kontexmenü angezeigt werden:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Fensterbereichs den Abschnitt **Häufig verwendete Benutzerkonten**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Liste im Programm-Menü anzeigen**.

   Damit eine Liste der häufig verwendeten Benutzerkonten im Menü der Titelleisten-Schaltfläche angezeigt wird, aktivieren Sie das Kontrollkästchen **Im Menü der Titelleisten-Schaltfläche anzeigen**.

   > Wenn das Kontrollkästchen **Liste im Programm-Menü anzeigen** deaktiviert ist, stehen die übrigen Einstellungen der Liste nicht für Änderungen zur Verfügung.

5. Geben Sie im Feld **Größe der Liste** die Anzahl der Benutzerkonten an.
6. Bei Bedarf können Sie die Liste manuell anpassen. Um ein Element aus der Liste zu löschen, markieren Sie darin das entsprechende Benutzerkonto und klicken Sie auf **Löschen**. Um alle Elemente aus der Liste zu löschen, klicken Sie auf **Leeren**.

IGNORIERTE WEBADRESSEN

Sie können eine Liste mit Webadressen anlegen, für die die Funktionen von Kaspersky Password Manager nicht verwendet werden. Für Webseiten aus dieser Liste wird die Funktion zum automatischen Ausfüllen von Kennwort und Benutzername deaktiviert. Außerdem schlägt Kaspersky Password Manager für diese Seiten nicht automatisch vor, ein neues Benutzerkonto (S. S. 24) / Benutzername zu (s. S. 29) erstellen.

➡ *Gehen Sie folgendermaßen vor, um eine Liste mit ignorierten Webadressen anzulegen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.

3. Wählen Sie im linken Fensterbereich den Abschnitt **Ignorierte Webadressen**.

4. Klicken Sie auf der rechten Fensterseite auf **Hinzufügen**, geben Sie dann eine Webadresse ein und drücken Sie die **EINGABE**-Taste.

   Um eine Webadresse zu ändern, markieren Sie sie in der Liste und klicken Sie auf **Ändern**. Um eine Webadresse aus der Liste zu löschen, markieren Sie sie und klicken Sie auf **Löschen**.

VERTRAUENSWÜRDIGE WEBADRESSEN

Kaspersky Password Manager bietet Ihren persönlichen Daten Schutz vor Phishing-Attacken. Wenn Sie bei einem Authentifizierungsversuch auf eine andere Webseite umgeleitet werden, informiert das Programm Sie darüber.

Häufig verwenden Angreifer eine Weiterleitung auf Webseiten, die den Zugriff auf Bankkonten ermöglichen (es kann sich beispielsweise um Seiten von Internet-Banken, Zahlungssysteme usw. handeln). Auf der Authentifizierung der offiziellen Webseite einer Firma wird eine Weiterleitung auf eine gefälschte Webseite eingerichtet, die der offiziellen Internetseite visuell gleicht. Alle auf der gefälschten Seite eingegebenen Daten gelangen in die Hände der Angreifer.

Viele Webseiten enthalten ganz legale Weiterleitungen. Damit Kaspersky Password Manager eine solche Weiterleitung nicht als Phishing-Attacke bewertet, können Sie eine Liste mit vertrauenswürdigen Webadressen anlegen. In die Liste der vertrauenswürdigen Webadressen werden Webadressen eingetragen, an die eingegebene persönliche Daten weitergeleitet werden. Kaspersky Password Manager meldet bei der Authentifizierung nicht, wenn persönliche Daten an eine vertrauenswürdige Webseite weitergeleitet werden.

Kaspersky Password Manager erlaubt die Weiterleitung persönlicher Daten von anderen Webseiten an eine vertrauenswürdige Webseite. Bevor Sie eine Webseite zur vertrauenswürdigen Liste hinzufügen, vergewissern Sie sich, dass sie vollkommen sicher ist.

Es bestehen folgende Möglichkeiten, um eine Webseite zur Liste der vertrauenswürdigen Webadressen hinzuzufügen:

- direkt bei der Authentifizierung auf einer Webseite
- manuell aus dem Fenster **Einstellungen von Kaspersky Password Manager**.

Um eine Webseite während der Authentifizierung zur Liste der vertrauenswürdigen Webadressen hinzuzufügen, warten Sie auf die Weiterleitung zu einer anderen Webseite und aktivieren Sie im folgenden Fenster von Kaspersky Password Manager das Kontrollkästchen **<Name der Webseite> immer vertrauen**.

➡ *Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Adressen manuell anzulegen:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im folgenden Fenster **Einstellungen**.

3. Wählen Sie im linken Fensterbereich den Abschnitt **Vertrauenswürdige Webadressen**.

4. Klicken Sie auf der rechten Fensterseite auf **Hinzufügen**. In der Liste **Vertrauenswürdige Webadressen** wird ein Feld eingeblendet. Geben Sie die Webadresse ein und drücken Sie die **EINGABE**-Taste.

   Um eine Webadresse zu ändern, markieren Sie sie in der Liste und klicken Sie auf **Ändern**. Um eine Webadresse aus der Liste zu löschen, markieren Sie sie und klicken Sie auf **Löschen**.

TASTENKOMBINATION

Um schnell und bequem auf bestimmte Programmfunktionen zuzugreifen, können Tastenkombinationen verwendet werden.

Für folgende Aktionen können Tastenkombinationen festgelegt werden:

- Kaspersky Password Manager blockieren / freigeben (s. S. 22).
- Kennwort eingeben

Für einen schnellen Funktionsaufruf können eine Taste oder Kombination aus zwei oder drei Tasten festgelegt werden.

Vermeiden Sie es, den Funktionen des Kaspersky Password Managers die Tastenkombinationen zuzuweisen, die bereits für Microsoft Windows verwendet werden.

Gehen Sie folgendermaßen vor, um Tastenkombinationen festzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Kaspersky Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Fensterbereich den Abschnitt **Tastenkombinationen**.
5. Legen Sie im rechten Fensterbereich die für eine Aktion gewünschte Tastenkombination fest.

ORT DER KENNWORT-DATENBANK

Die Kennwort-Datenbank von Kaspersky Password Manager ist eine verschlüsselte Datei (s. S. 42), in der alle Ihre persönlichen Daten (Benutzerkonten, Benutzernamen, Kennwörter und Visitenkarten) gespeichert sind.

In den einzelnen Versionen von Microsoft Windows gelten folgende Standardpfade für die Kennwort-Datenbank:

- für Microsoft Windows XP: C:\Dokumente und Einstellungen\Benutzername\Eigene Dateien\Passwords Database\
- für Microsoft Windows Vista: C:\Benutzer\Benutzername\Dokumente\Passwords Database
- für Microsoft Windows 7: C:\Benutzer\Benutzername\Dokumente\Passwords Database

Sie können als Speicher für Ihre Kennwort-Datenbank unterschiedliche Datenträger verwenden: Wechseldatenträger, lokaler Datenträger oder Netzlaufwerk.

Wenn der Pfad oder der Name der Kennwort-Datenbank geändert wird, bestehen folgende Varianten für das Vorgehen:

- **Kopieren** – Am angegebenen Pfad wird eine Kopie der Kennwort-Datenbank angelegt. Die Kopie wird zur aktiven Kennwort-Datenbank.
- **Verschieben** – Die aktive Kennwort-Datenbank wird am angegebenen Pfad gespeichert.
- **Neue Kennwort-Datenbank erstellen** – Es wird eine leere Kopie der Kennwort-Datenbank erstellt, die zur aktiven Datenbank wird.

Gehen Sie folgendermaßen vor, um eine Kennwort-Datenbank zu verschieben oder umzubenennen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Linkrogrammhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.
4. Klicken Sie auf der rechten Fensterseite im Block **Pfad** auf die Schaltfläche , die sich auf der rechten Seite des Felds **Pfad** befindet.
5. Geben Sie im folgenden Fenster **Kennwort-Datenbank auswählen** den Pfad und den Namen der Datei an, und klicken Sie anschließend auf **Öffnen**.
6. Wählen Sie im folgenden Fenster **Ort der Kennwort-Datenbank** die gewünschte Aktion für die Kennwort-Datenbank.
7. Geben Sie im folgenden Fenster **Kaspersky Password Manager** das Master-Kennwort ein, um die Änderungen zu bestätigen.

Gehen Sie folgendermaßen vor, um die aktuelle Kennwort-Datenbank zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.
4. Klicken Sie auf der rechten Fensterseite im Block **Pfad** auf die Schaltfläche , die sich auf der rechten Seite des Felds **Pfad** befindet.
5. Wählen Sie im folgenden Fenster **Kennwort-Datenbank auswählen** die Datei der Kennwort-Datenbank und klicken Sie auf **Öffnen**.
6. Geben Sie im folgenden Fenster **Kaspersky Password Manager** das Master-Kennwort ein, das für den Zugriff auf die ausgewählte Kennwort-Datenbank gilt.

NEUE KENNWORT-DATENBANK ANLEGEN

Kaspersky Password Manager erlaubt es, nacheinander mit mehreren Kennwort-Datenbanken zu arbeiten. Durch das Erstellen einer neuen Kennwort-Datenbank lassen sich Ihre persönlichen Daten aufteilen, indem sie in zwei oder mehr Kennwort-Datenbanken gespeichert werden. Bei Bedarf kann eine alte Kennwort-Datenbank wiederhergestellt werden. Kaspersky Password Manager schlägt vor, eine neue Kennwort-Datenbank zu erstellen, wenn die aktuelle Datenbank beschädigt wurde oder eine Wiederherstellung aus einer Sicherungskopie nicht möglich ist.

Gehen Sie folgendermaßen vor, um eine neue Kennwort-Datenbank zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.
4. Klicken Sie auf der rechten Fensterseite im Block **Pfad** auf die Schaltfläche , die sich auf der rechten Seite des Felds **Pfad** befindet.
5. Geben Sie im folgenden Fenster **Kennwort-Datenbank auswählen** einen Speicherort und einen Namen für die Datei der Kennwort-Datenbank an, und klicken Sie dann auf **Öffnen**.

6. Wählen Sie im folgenden Fenster **Ort der Kennwort-Datenbank** die Aktion **Neue Kennwort-Datenbank erstellen** aus.

7. Geben Sie im Fenster **Neue Kennwort-Datenbank** im Block **Kennwort** ein Kennwort für den Zugriff auf die neue Datenbank an und wiederholen Sie es im Feld **Kennwort bestätigen**.

   Wenn die Wiederholung des Kennworts falsch ist, wird sie rot hervorgehoben.

   Wählen Sie im Block **Verschlüsselungsalgorithmus** einen Cryptographic Service Provider und die gewünschte Verschlüsselungsmethode (s. S.42).

8. Geben Sie im folgenden Fenster ein neues Master-Kennwort ein, um das Erstellen einer neuen Kennwort-Datenbank zu bestätigen.

SPEICHERORT FÜR EINE SICHERUNGSKOPIE

Bevor irgendwelche Änderungen Ihrer persönlichen Daten gespeichert werden, legt Kaspersky Password Manager automatisch Sicherungskopien der Kennwort-Datenbank an. Dadurch wird erlaubt, im Fall von Systemabbrüchen oder technischen Störungen einen Datenverlust zu vermeiden. Kaspersky Password Manager erstellt eine vollständige Kopie der Kennwort-Datenbank. Die Kopie entspricht dem Zustand vor dem Speichern der letzten Änderungen.

Wenn eine Kennwort-Datenbank beschädigt wurde, können Sie die Daten aus der letzten Sicherungskopie der Kennwort-Datenbank wiederherstellen (s. S. 34).

Als Speicher für die Sicherungskopien der Kennwort-Datenbank kann ein Wechseldatenträger, lokaler Datenträger oder Netzlaufwerk.

Die Sicherungskopien werden abhängig vom Typ des Betriebssystems standardmäßig unter folgendem Pfad gespeichert:

- für Microsoft Windows XP: C:\Dokumente und Einstellungen\Benutzername\Eigene Dateien\Passwords Database
- für Microsoft Windows Vista: C:\Benutzer\Benutzername\Dokumente\Passwords Database
- für Microsoft Windows 7: C:\Benutzer\Benutzername\Dokumente\Passwords Database

Gehen Sie folgendermaßen vor, um den Pfad für Sicherungskopien zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.
4. Klicken Sie auf der rechten Fensterseite im Block **Backup** auf die Schaltfläche , die sich auf der rechten Seite des Felds **Pfad** befindet.
5. Wählen Sie im folgenden Fenster **Ordner suchen** den Zielordner für die Sicherungskopien der Kennwort-Datenbank.

VERSCHLÜSSELUNGSMETHODE AUSWÄHLEN

Die Aufgabe der Kryptographie besteht im Schutz von Informationen vor unbefugtem Zugriff und unerlaubter Verbreitung. Die Hauptfunktion einer Chiffre besteht darin, eine verschlüsselte Nachricht über einen ungeschützten Kanal zu senden.

Für die Verschlüsselung und Entschlüsselung werden Schlüssel benötigt. Ein Schlüssel ist ein obligatorischer Parameter einer Chiffre. Erfolgen Verschlüsselung und Entschlüsselung mit dem gleichen Schlüssel, so handelt es sich um einen symmetrischen Algorithmus. Werden zwei Schlüssel eingesetzt, dann ist der Algorithmus asymmetrisch. Bei symmetrischen Chiffren wird zwischen Block- und Stromchiffrierung unterschieden. Eine beliebige Information wird (unabhängig vom Format der Ausgangsdaten) als binärer Code interpretiert. Bei der Blockverschlüsselung werden alle Daten in Blöcke unterteilt, die dann voneinander unabhängig verschlüsselt werden. Bei der Stromverschlüsselung werden Informationen bitweise chiffriert.

Kaspersky Password Manager bietet folgende symmetrische Verschlüsselungsalgorithmen:

- **DES**. Blockverschlüsselung mit einer standardmäßigen Schlüsselgröße von 56 Bit. Nach heutigen Maßstäben bietet DES kein hohes Schutzniveau. Der Algorithmus wird verwendet, wenn keine hohen Sicherheitsanforderungen gelten.
- **3DES**. Blockverschlüsselung, die auf DES beruht. Der größte Nachteil des vorhergehenden Algorithmus, die geringe Schlüsselgröße, wurde hier behoben. Die Schlüsselgröße ist für 3DES dreimal größer als für DES (56*3=168 Bit). Die Funktionsgeschwindigkeit ist dreimal geringer als bei DES, dafür ist die Sicherheit erheblich höher. 3DES wird häufiger verwendet, weil DES keine ausreichende Stabilität gegen die heutzutage verwendeten Technologien zum "Knacken" von Chiffren besitzt.
- **3DES TWO KEY**. Blockverschlüsselung, die auf DES beruht. Ein Algorithmus des Typs 3DES, für den die Schlüsselgröße 112 Bit beträgt (56*2).
- **RC2**. Blockverschlüsselung mit variabler Schlüssellänge mit relativ hoher Verarbeitungsgeschwindigkeit. Dieser Algorithmus ist schneller als DES. Im Hinblick auf Sicherheit und Stabilität gleicht er dem Algorithmus 3DES.
- **RC4**. Blockverschlüsselung mit variabler Schlüssellänge. Die Schlüsselgröße beträgt von 40 bis 256 Bit. Die Vorteile des Algorithmus liegen in der hohen Geschwindigkeit und der variablen Schlüsselgröße. Kaspersky Password Manager verwendet für die Datenverschlüsselung standardmäßig den Algorithmus RC4.
- **AES**. Symmetrischer Blockverschlüsselungsalgorithmus mit einer Schlüsselgröße von 128, 192 oder 256 Bit. Der Algorithmus garantiert ein hohes Sicherheitsniveau und genießt höchste Popularität.

Um im Betriebssystem Microsoft Windows Verschlüsselungsoperation auszuführen, wird ein Cryptographic Provider verwendet. Jeder Cryptographic Provider unterstützt mehrere Verschlüsselungsalgorithmus mit unterschiedlicher Schlüssellänge. Kaspersky Password Manager verwendet folgende in Microsoft Windows integrierte Cryptographic Provider:

- Microsoft Base Cryptographic Provider
- Microsoft Enhanced Cryptographic Provider
- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)
- Microsoft RSA/Schannel Cryptographic Provider
- Microsoft Strong Cryptographic Provider

➧ *Gehen Sie folgendermaßen vor, um den Verschlüsselungsalgorithmus zu ändern:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Kaspersky Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.

4. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.
5. Klicken Sie auf der rechten Fensterseite im Block **Verschlüsselung** auf **Ändern**.
6. Geben Sie im folgenden Fenster **Verschlüsselungsalgorithmus** die Verschlüsselungseinstellungen an.

KENNWORT-DATENBANK AUTOMATISCH BLOCKIEREN

Nach dem Programmstart und nach Ablauf eines festgelegten Zeitraums, während dem der Computer inaktiv war, blockiert Kaspersky Password Manager die Kennwort-Datenbank automatisch. Sie können eine Zeitspanne festlegen, nach deren Ablauf die Kennwort-Datenbank blockiert werden soll. Der Wert des Intervalls kann zwischen 1 und 60 Minuten liegen. Es wird empfohlen, für das Blockieren der Kennwort-Datenbank einen Wert von 5-20 Minuten Inaktivität des Computers festzulegen. Sie können auch das automatische Blockieren der Kennwort-Datenbank deaktivieren.

Nach einer bestimmten Inaktivitätsdauer des Computers blockiert Kaspersky Password Manager die Kennwort-Datenbank automatisch. Wenn das automatische Blockieren des Computers deaktiviert wird, sind Ihre persönlichen Daten ungeschützt, wenn Sie sich vom Computer entfernen, ohne ihn zuvor manuell zu sperren.

Gehen Sie folgendermaßen vor, um den Zeitraum zu ändern, nach dem die Kennwort-Datenbank blockiert wird:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.
4. Wählen Sie auf der rechten Fensterseite im Block **Automatisches Blockieren** aus der Dropdown-Liste eine Inaktivitätsdauer des Computers, nach deren Ablauf die Kennwort-Datenbank blockiert werden soll.

   Um das Blockieren der Kennwort-Datenbank zu deaktivieren, wählen Sie den Wert **Nie**.

AUTHENTIFIZIERUNGSMETHODE FÜR KASPERSKY PASSWORD MANAGER ÄNDERN

Die Authentifizierung erlaubt es, den Zugriff auf Ihre persönlichen Daten zu kontrollieren. Die Authentifizierungsmethode wird beim ersten Start von Kaspersky Password Manager ausgewählt. Die Authentifizierungsmethode kann aber später geändert werden.

Gehen Sie folgendermaßen vor, um die Authentifizierungsmethode zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Login-Methode**.
4. Wählen Sie auf der rechten Fensterseite im Block **Login-Methode** in der Dropdown-Liste eine Authentifizierungsmethode.

SIEHE AUCH:

USB- oder Bluetooth-Geräte zur Authentifizierung verwenden 45

USB- ODER BLUETOOTH-GERÄTE ZUR AUTHENTIFIZIERUNG VERWENDEN

Für den Zugriff auf die Kennwort-Datenbank (s. S. 44) erlaubt Kaspersky Password Manager die Verwendung unterschiedlicher USB- und Bluetooth-Geräte.

➡ *Gehen Sie folgendermaßen vor, um für den Zugriff auf die Kennwort-Datenbank ein USB-Gerät zu verwenden:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Login-Methode**.
4. Wählen Sie auf der rechten Fensterseite im Block **Login-Methode** in der Dropdown-Liste den Wert **USB-Gerät**.
5. Schließen Sie das tragbare Gerät an den Computer an.
6. Wählen Sie aus der Liste **Laufwerke** ein Gerät und klicken Sie auf **Installieren**. Neben dem ausgewählten Gerät erscheint das Symbol ✓. Wenn das angeschlossene Gerät nicht auf der Liste steht, aktivieren Sie das Kontrollkästchen **Zusätzliche Geräte anzeigen**. Bei Bedarf können Sie das Authentifizierungsgerät durch Klick auf **Zurücksetzen** ändern.

➡ *Gehen Sie folgendermaßen vor, um für den Zugriff auf die Kennwort-Datenbank ein Bluetooth-Gerät zu verwenden:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Login-Methode**.
4. Wählen Sie auf der rechten Fensterseite im Block **Login-Methode** in der Dropdown-Liste den Wert **Bluetooth-Gerät**.
5. Aktivieren Sie die Bluetooth-Funktion zuerst auf Ihrem Computer und dann auf dem Gerät.
6. Wählen Sie ein Gerät aus der Liste **Telefone und Modems** und klicken Sie dann auf **Installieren**. Neben dem ausgewählten Gerät erscheint das Symbol ✓. Bei Bedarf kann das Authentifizierungsgerät durch Klick auf **Zurücksetzen** geändert werden.

MASTER-KENNWORT ÄNDERN

Das Master-Kennwort wird beim ersten Start von Kaspersky Password Manager festgelegt. Es kann später geändert werden.

Bei einer Änderung des Master-Kennworts fordert Kaspersky Password Manager eine Bestätigung des eingegebenen Kennworts (wiederholte Eingabe des neuen Kennworts). Es ist nicht möglich, ein neues Kennwort ohne Bestätigung zu speichern. Wenn das eingegebene Kennwort und seine Wiederholung voneinander abweichen, wird die Wiederholung des Kennworts rot hervorgehoben. Beim Versuch das neue Kennwort zu speichern, erfolgt in diesem Fall ein Warnhinweis.

➡ *Gehen Sie folgendermaßen vor, um das Master-Kennwort zu ändern:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.

3. Wählen Sie im linken Fensterbereich den Abschnitt **Login-Methode**.
4. Klicken Sie auf der rechten Fensterseite im Block **Kennwortschutz** auf **Ändern**.
5. Tragen Sie das neue Kennwort im folgenden Fenster **Kennwortschutz** in die Felder **Kennwort** und **Kennwort bestätigen** ein.

UNTERSTÜTZTE WEBBROWSER

Damit die Funktionen zur automatischen Aktivierung eines Benutzerkontos und die Titelleisten-Schaltflächen (s. S. 49) korrekt arbeiten, fordert Kaspersky Password Manager für bestimmte Webbrowser die Installation zusätzlicher Erweiterungen (Plug-ins). In der Grundeinstellung erfolgt die Installation von Erweiterungen beim ersten Start von Kaspersky Password Manager. Sie können zusätzlich ein erforderliches Plug-in installieren.

Der Kaspersky Password Manager bietet eine Liste der Webbrowser und Mailprogramme, in der jedes Programm den Status **Installiert** / **Nicht installiert** besitzt, je nachdem, ob ein entsprechendes Plug-in installiert wurde oder nicht.

Es wird empfohlen, alle Programme, für die Sie ein Plug-in installieren möchten, zu schließen.

➡ *Gehen Sie folgendermaßen vor, um ein Plug-in für einen Webbrowser oder ein Mailprogramm zu installieren:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Unterstützte Webbrowser**.
4. Wählen Sie auf der rechten Fensterseite aus der Liste **Unterstützte Webbrowser und verfügbare Erweiterungen** ein Programm und klicken Sie dann auf **Installieren**.
5. Folgen Sie den Hinweisen des **Installationsassistenten**. Nachdem ein Plug-in installiert wurde, wird der Name des Programms automatisch in die Gruppe **Installierte** Webbrowser verschoben. Es erhält den Status **Installiert**. Zum Löschen von installierten Erweiterungen dient die Schaltfläche **Löschen**.

VORLAGEN FÜR PERSÖNLICHE NOTIZEN VERWALTEN

Sie können die vorgegebenen Vorlagen für persönliche Notizen (s. S. 30) bearbeiten, neue Vorlagen erstellen oder eine vorhandene persönliche Notiz als Vorlage verwenden.

➡ *Gehen Sie folgendermaßen vor, um eine vorgegebene Vorlage für eine persönliche Notiz zu ändern:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite den Abschnitt **Vorlagen verwalten**.
4. Wählen Sie im rechten Fensterbereich eine Vorlage aus der Liste aus und klicken Sie auf **Ändern**.
5. Nehmen Sie im Texteditor die erforderlichen Änderungen vor.

➡ *Gehen Sie folgendermaßen vor, um eine Vorlage für eine persönliche Notiz zu erstellen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite den Abschnitt **Vorlagen verwalten**.

4. Klicken Sie auf der rechten Fensterseite auf **Hinzufügen**.
5. Geben Sie im folgenden Fenster im Feld **Name** einen Namen für die neue Notiz-Vorlage ein.
6. Geben Sie die entsprechenden Informationen im Texteditor ein.

➡ *Gehen Sie folgendermaßen vor, um eine vorhandene persönliche Notiz als Vorlage zu verwenden:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Password Manager**.
3. Wählen Sie im folgenden Fenster die entsprechende Notiz aus der Liste aus und klicken Sie im oberen Fensterbereich auf **Ändern**.
4. Klicken Sie im folgenden Fenster unten auf **Als Vorlage speichern**.
5. Geben Sie im folgenden Fenster im Feld **Name** einen Namen für die neue Notiz-Vorlage ein.

ZEITPUNKT FÜR DEN PROGRAMMSTART

In der Grundeinstellung wird Kaspersky Password Manager beim Hochfahren des Betriebssystems gestartet. Sie können die Einstellungen für den Programmstart ändern.

➡ *Gehen Sie folgendermaßen vor, um das Programm manuell zu starten:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Allgemein**.
4. Deaktivieren Sie auf der rechten Fensterseite im Block **Allgemein** das Kontrollkästchen **Kaspersky Password Manager beim Hochfahren des Betriebssystems starten**.

AKTION BEI DOPPELKLICK

Kaspersky Password Manager erlaubt es, eine Aktion festzulegen, die bei Doppelklick auf das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows (s. S. 18) gestartet werden soll. Folgende Aktionen stehen zur Auswahl:

- Hauptfenster von Kaspersky Password Manager öffnen (s. S. 19).
- Kaspersky Password Manager blockieren / freigeben (Standardaktion).

➡ *Gehen Sie folgendermaßen vor, um die Aktion zu ändern, die durch Doppelklick auf das Programmsymbol im Infobereich der Taskleiste gestartet werden soll:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Allgemein**.
4. Wählen Sie auf der rechten Fensterseite in der Dropdown-Liste **Doppelklick auf das Symbol** eine Aktion.

MELDUNGEN

Bei der Arbeit von Kaspersky Password Manager treten unterschiedliche Arten von Ereignissen auf, die gewöhnlich informativen Charakter besitzen. Verwenden Sie den Benachrichtigungsdienst, um sich über Ereignisse informieren zu lassen. Der Benutzer wird durch Tool-Tipps und Popup-Meldungen informiert.

Im Programm gibt es folgende Typen von Benachrichtigungen:

- **Programm starten**. Die Meldung erfolgt bei einem wiederholten Programmstart, wenn das Programm bereits gestartet und die Kennwort-Datenbank nicht blockiert wurde.
- **Benutzerkonto aktivieren**. Die Meldung erfolgt, wenn ein Benutzerkonto aktiviert wird.
- **Zwischenablage leeren**. Kaspersky Password Manager erlaubt es, ein Kennwort vorübergehend in der Zwischenablage zu speichern. Dadurch lassen sich Daten bequem kopieren und in ein ausgewähltes Feld einfügen. Nach Ablauf einer festgelegten Zeitspanne (s. S. 48) wird das Kennwort aus der Zwischenablage gelöscht.
- **Kaspersky Password Manager automatisch blockieren**. Wenn Kaspersky Password Manager automatisch die Kennwort-Datenbank blockiert, erscheint eine Meldung. Die Kennwort-Datenbank wird nach dem Hochfahren des Betriebssystems und nach einem festgelegten Zeitraum (s. S. 44), während dem der Computer inaktiv war, automatisch blockiert.
- **Daten in eine ungeschützte Datei exportieren**. Warnmeldung, dass Ihre Kennwörter durch den Export in einer unverschlüsselten Datei gespeichert werden und dadurch jedem Benutzer, der auf Ihren Computer arbeitet, zugänglich sind. Es wird empfohlen, vor dem Export zu überlegen, wie die Datei mit den Kennwörtern geschützt werden kann.
- **Formular manuell ändern**. Um die Einstellungen von Zusatzfeldern anzupassen, fragt das Programm nach der Erlaubnis, den standardmäßig installierten Webbrowser zu verwenden. Die Meldung warnt davor, dass Bilder und Systemdateien (Cookies) auf Ihrem Computer gespeichert werden.
- **Probleme beim Ausfüllen eines Benutzernamens für ein Benutzerkonto**. Die Meldung warnt davor, dass es nicht möglich ist, bei der Authentifizierung automatisch Daten einzufügen.

➡ *Gehen Sie folgendermaßen vor, um Meldung erhalten:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Allgemein**.
4. Klicken Sie auf der rechten Fensterseite im Block **Allgemein** auf **Meldungseinstellungen**.
5. Aktivieren / deaktivieren Sie im folgenden Fenster das Kontrollkästchen für die entsprechenden Benachrichtigungstypen.

SPEICHERDAUER DES KENNWORTS IN DER ZWISCHENABLAGE

Kaspersky Password Manager erlaubt es, ein Kennwort für einen festgelegten Zeitraum in der Zwischenablage zu speichern. Diese Option ist nützlich, um schnell mit Kennwörtern zu arbeiten (beispielsweise wenn es erforderlich ist, ein erstelltes Kennwort bei der Anmeldung auf einer Webseite / in einem Programm zu verwenden). Sie können den Zeitraum festlegen, für den ein Kennwort in der Zwischenablage gespeichert werden soll. Nach Ablauf dieses Zeitraums wird das Kennwort automatisch aus der Zwischenablage gelöscht. Dies verhindert das Abfangen und den Diebstahl von Kennwörtern, weil ein Kennwort nach dem festgelegten Zeitraum nicht mehr aus der Zwischenablage kopiert werden kann.

➡ *Gehen Sie folgendermaßen vor, um festzulegen, wie lange ein Kennwort in der Zwischenablage gespeichert werden soll:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Allgemein**.
4. Legen Sie auf der Rechten Fensterseite im Block **Zwischenablage** eine Dauer in Sekunden fest.

TITELLEISTEN-SCHALTFLÄCHE ANZEIGEN

Wenn in ein Programm, mit dem Sie arbeiten, nicht nur das Menü von Kaspersky Password Manager, sondern auch Menüs anderer Programme integriert sind, können Sie die Position der Titelleisten-Schaltfläche im Verhältnis zu anderen Schaltflächen ändern. Außerdem kann manuell eine Liste der Webbrowser angelegt werden, für die eine Titelleisten-Schaltfläche (s. S. 21) verwendet werden soll.

➡ *Gehen Sie folgendermaßen vor, um die Einstellungen für die Anzeige der Titelleisten-Schaltfläche zu ändern:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster **Einstellungen**.
3. Wählen Sie im linken Bereich des Fensters den Abschnitt **Titelleisten-Schaltfläche**.
4. Passen Sie auf der rechten Fensterseite im Block **Titelleisten-Schaltfläche anzeigen** die erforderlichen Parameter in Abhängigkeit von der Aufgabe an:
   - Um die Position der Titelleisten-Schaltfläche zu ändern, geben Sie im Feld **Schaltfläche nach links verschieben** eine Positionsnummer für die Schaltfläche ein (wie weit die Titelleisten-Schaltfläche nach links verschoben werden soll).
   - Damit die Titelleisten-Schaltfläche nicht angezeigt wird, wenn die Kennwort-Datenbank blockiert ist, aktivieren Sie das Kontrollkästchen **Nicht anzeigen, wenn Kaspersky Password Manager blockiert wurde**.
   - Um eine Liste der Webbrowser anzulegen, in die die Titelleisten-Schaltfläche integriert werden soll, aktivieren Sie im Block **Titelleisten-Schaltfläche in folgenden Webbrowsern anzeigen** das Kontrollkästchen für die entsprechenden Webbrowser.

ERSTELLEN VON SICHEREN KENNWÖRTERN

Die Datensicherheit ist direkt von der Stärke der Kennwörter abhängig. In folgenden Fällen können Daten einem Risiko unterliegen:

- Es wird für alle Benutzerkonten das gleiche Kennwort benutzt.
- Es wird ein zu einfaches Kennwort verwendet.
- Als Kennwort werden Informationen verwendet, die sich leicht erraten lassen (z.B. Namen von Familienmitgliedern oder ihre Geburtstage).

Um die Datensicherheit zu gewährleisten, besitzt Kaspersky Password Manager eine Funktion, mit der unter Verwendung eines Kennwort-Generators einzigartige und sichere Kennwörter für Benutzerkonten generiert werden können.

Ein Kennwort gilt als sicher, wenn es aus mehr als vier Zeichen besteht und Sonderzeichen, Ziffern, Groß- und Kleinbuchstaben darin verwendet werden.

Die Kennwortstärke wird durch folgende Parameter bestimmt:

- **Länge** – Anzahl der Zeichen in einem Kennwort. Der Wert kann zwischen 4 und 99 Zeichen liegen. Je länger ein Kennwort ist, desto sicherer ist es.
- **A-Z** – Verwendung von Großbuchstaben.
- **a-z** – Verwendung von Kleinbuchstaben.
- **0-9** – Verwendung von Ziffern.
- **Sonderzeichen** – Verwendung von Sonderzeichen.
- **Zeichen nicht doppelt verwenden** – Verbot der Verwendung von gleichen Zeichen in einem Kennwort.

➧ *Gehen Sie folgendermaßen vor, um mit dem Kennwort-Generator ein sicheres Kennwort zu erstellen:*

1. Öffnen Sie das Kontextmenü von Kaspersky Password Manager und wählen Sie den Punkt **Kennwort-Generator**.
2. Geben Sie im folgenden Fenster **Kennwort-Generator** im Feld **Länge des Kennworts** die Anzahl der Zeichen im Kennwort an.
3. Passen Sie bei Bedarf zusätzliche Einstellungen für den Kennwort-Generator an. Aktivieren / deaktivieren Sie dazu im Block **Erweiterte Einstellungen** das Kontrollkästchen der entsprechenden Parameter.
4. Klicken Sie auf **Generieren**. Das erstellte Kennwort wird im Feld **Kennwort** angezeigt. Um das generierte Kennwort zu lesen, aktivieren Sie das Kontrollkästchen **Kennwort anzeigen**.
5. Kopieren Sie das Kennwort mit der Schaltfläche in die Zwischenablage und fügen Sie es dann mit der Tastenkombination **STRG+V** in einem Programm / auf einer Webseite ein. Das erstellte Kennwort wird in der Zwischenablage gespeichert.
6. Aktivieren Sie das Kontrollkästchen **Standard**, um die ausgewählten Einstellungen zur späteren Verwendung zu speichern.

VERWENDUNG EINER PORTABLEN VERSION DES KASPERSKY PASSWORD MANAGERS

Kaspersky Password Manager erlaubt es, alle Kennwörter auf einem Wechseldatenträger zu speichern (z.B. auf einer Speicherkarte oder auf einem Mobiltelefon, wenn es als Speicherkarte verwendet wird). Dazu ist es erforderlich, auf einem Wechseldatenträger eine portable Version des Kaspersky Password Managers zu erstellen. Die portable Programmversion wird auf Ihrem Computer erstellt, auf dem die Vollversion von Kaspersky Password Manager installiert ist. Die portable Programmversion besitzt die vollständige Funktionalität von Kaspersky Password Manager.

Die portable Version erlaubt es, den Kaspersky Password Manager auf einem allgemein zugänglichen Computer zu verwenden (z.B. im Internet-Café oder in einer Bibliothek), auf dem Kaspersky Password Manager nicht installiert ist. Wenn der Wechseldatenträger mit dem Computer verbunden wird, startet Kaspersky Password Manager automatisch. Sobald der Wechseldatenträger getrennt wird, schließt sich Kaspersky Password Manager automatisch und Ihre Daten verbleiben nicht auf dem öffentlichen Computer.

Außerdem können Sie mit Hilfe der portablen Version Ihre Kennwort-Datenbanken synchronisieren, wenn Kaspersky Password Manager installiert ist und parallel auf verschiedenen Computern verwendet wird (z.B. zuhause und im Büro).

IN DIESEM ABSCHNITT

PORTABLE VERSION ERSTELLEN UND VERBINDEN

Um zu gewährleisten, dass die portable Version des Kaspersky Password Managers auf einem öffentlich zugänglichen Computer richtig funktioniert, wird empfohlen, die zusätzlichen Plug-ins für den Webbrowser zu installieren.

Ein Plug-in kann auf eine der folgenden Arten installiert werden:

- Aus dem Fenster des Assistenten zur Plug-in-Installation. Folgen Sie dazu beim ersten Start der portablen Version von Kaspersky Password Manager den Anweisungen des Assistenten zur Plug-in-Installation.
- Aus dem Menü der Titelleisten-Schaltfläche im Fenster des Webbrowsers. Wählen Sie dazu im Menü der Titelleisten-Schaltfläche den Punkt **Autoausfüllen-Plug-in nicht installiert** aus.

Beim ersten Start auf einem öffentlichen Computer wird automatisch der Installationsassistent für die portable Version von Kaspersky Password Manager gestartet.

Ihnen wird angeboten, folgende Zusatzeinstellungen für die Verwendung der portablen Programmversion festzulegen:

- Verknüpfung auf Desktop erstellen - Mit dieser Verknüpfung kann das Programm künftig vom Desktop des Computers aus gestartet werden.
- Virtuelle Tastatur verwenden – Öffnet die virtuelle Tastatur zur Eingabe von persönlichen Daten.

Gehen Sie folgendermaßen vor, um eine portable Version des Passwort-Managers zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im folgenden Fenster auf **Portable Version**.

3. Wählen Sie im folgenden Fenster das Gerät aus, auf das Sie die portable Version von **Kaspersky Password Manager** installieren wollen, und klicken Sie auf **Weiter**.

4. Legen Sie im folgenden Fenster die Einstellungen für die portable Version fest:

   - Um das Master-Kennwort für den Zugriff auf die portable Version von Kaspersky Password Manager nicht einzugeben, aktivieren Sie das Kontrollkästchen **Nie nach Master-Kennwort fragen**.

   - Damit die portable Version automatisch gestartet wird, wenn der Wechseldatenträger mit einem Computer verbunden wird, aktivieren Sie das Kontrollkästchen **Autostart von Password Manager von einem portablen Gerät aktivieren**.

5. Klicken Sie auf **Ausführen**. Klicken Sie nach dem Abschluss der Installation auf **Fertig**.

Gehen Sie folgendermaßen vor, um die portable Programmversion zu verwenden:

1. Schließen Sie den Wechseldatenträger an den Computer an.

2. Starten Sie die portable Version von Kaspersky Password Manager von dem ausgewählten Wechseldatenträger, falls diese beim Anschließen des Datenträgers nicht automatisch gestartet wurde.

3. Beim ersten Start der portablen Version wird Ihnen vorgeschlagen, die Autoausfüllen-Plug-ins zu installieren und die Kennwort-Manager zu deaktivieren, die in den auf Ihrem Computer installierten Webbrowsern integriert sind.

4. Geben Sie im folgenden Fenster das Master-Kennwort ein.

   Die portable Version des Kaspersky Password Managers ist zur Verwendung bereit.

SYNCHRONISIERUNG DER KENNWORT-DATENBANK

Wenn Sie den Kaspersky Password Manager auf unterschiedlichen Computern einsetzen, ist es erforderlich, alle Kennwort-Datenbanken aktuell zu halten. Mit der portablen Programmversion können Sie die Daten synchronisieren und auf allen Computern, auf denen der Kaspersky Password Manager installiert ist, die aktuelle Kennwort-Datenbank verwenden. Synchronisieren Sie dazu die Kennwort-Datenbank der portablen Version mit der Kennwort-Datenbank auf einem der Computer und wiederholen Sie die Synchronisierung dann auf einem anderen Computer.

Gehen Sie folgendermaßen vor, um die Kennwort-Datenbank der portablen Version mit der Kennwort-Datenbank auf einem der Computer zu synchronisieren:

1. Schließen Sie den Wechseldatenträger an den Computer an.

2. Öffnen Sie das Programmhauptfenster.

3. Klicken Sie im folgenden Fenster auf **Portable Version**.

4. Wählen Sie im folgenden Fenster das Gerät aus, auf dem die portable Version des Kaspersky Password Managers installiert ist, und klicken Sie auf **Weiter**.

5. Wählen Sie im folgenden Fenster eine Synchronisierungsmethode für die Kennwort-Datenbank aus:

   - Um die Daten aus der Datenbank des Kaspersky Password Managers, der auf dem Computer installiert ist, zur Kennwort-Datenbank der portablen Version hinzuzufügen, wählen Sie die Variante **Kennwort-Datenbanken zusammenführen** aus

     Die Datenbank des Kaspersky Password Managers auf dem Computer bleibt dabei unverändert. Um die zusammengeführten Daten in diese Datenbank aufzunehmen, wiederholen Sie die Synchronisierung und wählen Sie die Variante **Kennwort-Datenbank der portablen Version verwenden**.

- Um die Kennwort-Datenbank der portablen Version durch die Datenbank des auf dem Computer installierten Kaspersky Password Managers zu ersetzen, wählen Sie in der portablen Version die Variante **Datenbank des auf dem Computer installierten Kaspersky Password Managers verwenden** aus.
- Um die Datenbank des auf dem Computer installierten Kaspersky Password Managers durch die Kennwort-Datenbank der portablen Version zu ersetzen, wählen Sie die Variante **Kennwort-Datenbank der portablen Version verwenden** aus.

6. Klicken Sie auf **Weiter**.
7. Legen Sie im folgenden Fenster die Einstellungen für die portable Version fest:
   - Um das Master-Kennwort für den Zugriff auf die portable Version von Kaspersky Password Manager nicht einzugeben, aktivieren Sie das Kontrollkästchen **Nie nach Master-Kennwort fragen**.
   - Damit die portable Version automatisch gestartet wird, wenn der Wechseldatenträger mit einem Computer verbunden wird, aktivieren Sie das Kontrollkästchen **Autostart von Password Manager von einem portablen Gerät aktivieren**.
8. Klicken Sie auf **Ausführen**. Klicken Sie nach dem Abschluss der Synchronisierung auf **Fertig**.

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an: Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Die Zentrale befindet sich in Russland, es gibt Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Benelux-Ländern, China, Polen, Rumänien und in den USA (Kalifornien). In Frankreich wurde eine neue Tochtergesellschaft gegründet, das Europäische Zentrum für Antiviren-Forschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das sind heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome und sechzehn einen Doktortitel besitzen. Die führenden Virusanalytiker von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens sind das einzigartige Wissen und die Erfahren, die die Mitarbeiter im Laufe des mehr als vierzehnjährigen ununterbrochenen Kampfes gegen Viren gesammelt haben. Dank der ständigen Analyse von Virenaktivitäten können wir Tendenzen bei der Malware-Entwicklung vorhersagen und frühzeitig Benutzern einen zuverlässigen Schutz vor neuen Angriffen an die Hand geben. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab. Wir sind unseren Wettbewerbern stets einen Schritt voraus und bieten unseren Kunden den besten Schutz.

Aufgrund der jahrelangen Tätigkeit wurde das Unternehmen zum führenden Entwickler von Technologien zum Schutz vor Viren. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Bequeme Steuerelemente versetzen die Benutzer in die Lage, den Antivirenschutz von Computern und Unternehmensnetzwerken maximal zu automatisieren. Viele internationale Developer verwendeten in ihrer Software den Kernel von Kaspersky Anti-Virus, beispielsweise: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir projektieren, realisieren und begleiten Antiviren-Komplex-Lösungen von Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Wir haben für unsere Benutzer einen technischen Kundendienst in mehreren Sprachen eingerichtet.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir beraten Sie gern detailliert über das Telefon oder E-Mail. Auf Ihre Fragen bekommen Sie eine vollständige und erschöpfende Antwort.

Webseite von Kaspersky Lab:	http://www.kaspersky.de
Viren-Enzyklopädie:	http://www.securelist.com/de/
Antiviren-Labor:	newvirus@kaspersky.com (nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de (für Fragen an die Virenanalytiker)
Webforum von Kaspersky Lab:	http://forum.kaspersky.com